Seguridad de vSphere

Actualización 2
Modificado el 28 abril de 2022
VMware vSphere 6.7
VMware ESXi 6.7
vCenter Server 6.7

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Acerca de la seguridad de vSphere 12

Información actualizada 15

1 Seguridad en el entorno de vSphere 18
Proteger hipervisor de ESXi 18
Proteger los sistemas vCenter Server y los servicios asociados 20
Proteger máquinas virtuales 22
Proteger la capa de redes virtuales 23
Contraseñas en el entorno de vSphere 25
Recursos y prácticas recomendadas de seguridad 26

2 Tareas de administración de permisos y usuarios de vSphere 28
Descripción de la autorización en vSphere 29
Herencia jerárquica de permisos 33
Configuración de varios permisos 36
Ejemplo 1: Herencia de permisos de varios grupos 36
Ejemplo 2: permisos secundarios que anulan permisos primarios 37
Ejemplo 3: función de usuario que anula la función de grupo 38
Administrar permisos para componentes de vCenter 38
Agregar un permiso a un objeto de inventario 39
Cambiar o quitar permisos 40
Cambiar la configuración de validación de usuarios 40
Permisos globales 41
Agregar permisos globales 42
Permisos en objetos de etiqueta 42
Usar funciones para asignar privilegios 44
Crear una función personalizada 46
Funciones del sistema vCenter Server 47
Prácticas recomendadas para funciones y permisos 48
Privilegios necesarios para la realización de tareas comunes 49

3 Proteger hosts ESXi 53
Recomendaciones generales sobre seguridad de ESXi 54
Configurar hosts ESXi con Host Profiles 55
Usar scripts para administrar las opciones de configuración de hosts 56
Bloqueo de cuenta y contraseñas ESXi 57
Seguridad de SSH 60

Claves SSH de ESXi 60
Dispositivos PCI/PCIe y ESXi 62
Deshabilitar el explorador de objetos administrados 63
Recomendaciones de seguridad para redes de ESXi 64
Modificar la configuración del proxy web de ESXi 64
Consideraciones de seguridad de vSphere Auto Deploy 65
Acceso de control para herramientas de supervisión de hardware basadas en CIM 66
Administrar certificados para hosts ESXi 67
Certificados y actualizaciones de hosts 70
Flujos de trabajo de cambio de modo de certificado 71
Configuración predeterminada de certificados ESXi 73
Cambiar configuración predeterminada de certificados 74
Ver la información de caducidad de certificados de varios hosts ESXi 75
Ver los detalles de certificado para un host único de ESXi 75
Renovar o actualizar de certificados de ESXi 76
Cambiar el modo de certificado 77
Reemplazo de certificados y claves SSL de ESXi 78
Requisitos de las solicitudes de firma de certificados de ESXi 79
Reemplazar el certificado y de la clave predeterminados de ESXi Shell 79
Reemplazo de la clave y el certificado predeterminados con el comando vifs 80
Reemplazar un certificado predeterminado mediante el método PUT de HTTPS 81
Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados) 82
Usar certificados personalizados con Auto Deploy 83
Restaurar archivos de certificados y claves de ESXi 85
Personalizar hosts con el perfil de seguridad 86
Configurar firewalls de ESXi 86
Administrar la configuración del firewall de ESXi 87
Agregar direcciones IP permitidas para un host ESXi 88
Puertos de firewall entrantes y salientes para hosts de ESXi 89
Comportamiento de firewall del cliente NFS 90
Comandos de firewall ESXCLI de ESXi 91
Personalizar los servicios de ESXi desde el perfil de seguridad 92
Habilitar o deshabilitar un servicio 93
Modo de bloqueo 95
Comportamiento del modo de bloqueo 95
Habilitar modo de bloqueo 97
Deshabilitar el modo de bloqueo 97
Habilitar o deshabilitar el modo normal de bloqueo desde la interfaz de usuario de la consola directa 98
Especificar cuentas con privilegios de acceso en el modo de bloqueo 99
Administrar los niveles de aceptación de hosts y VIB 101

Asignar privilegios para hosts ESXi 103
Usar Active Directory para administrar usuarios de ESXi 106
Configurar un host para utilizar Active Directory 106
Agregar un host a un dominio de servicio de directorio 107
Ver la configuración del servicio de directorio 108
Usar vSphere Authentication Proxy 108
Habilitar vSphere Authentication Proxy 109
Agregar un dominio a vSphere Authentication Proxy con vSphere Web Client 110
Agregar un dominio a vSphere Authentication Proxy con el comando camconfig 111
Usar vSphere Authentication Proxy para agregar un host a un dominio 112
Habilitar la autenticación de cliente para vSphere Authentication Proxy 113
Importar el certificado de vSphere Authentication Proxy en el host ESXi 114
Generar un nuevo certificado para vSphere Authentication Proxy 114
Configurar vSphere Authentication Proxy para usar certificados personalizados 115
Configurar la autenticación de tarjeta inteligente de ESXi 117
Habilitar la autenticación de tarjeta inteligente 118
Deshabilitar la autenticación de tarjeta inteligente 119
Autenticar con nombre de usuario y contraseña en caso de problemas de conectividad 119
Usar la autenticación de tarjeta inteligente en el modo de bloqueo 120
Usar ESXi Shell 120
Habilitar el acceso a ESXi Shell 121
Crear un tiempo de espera de disponibilidad de ESXi Shell 122
Crear un tiempo de espera para sesiones de ESXi Shell inactivas 123
Usar la interfaz de usuario de la consola directa para habilitar el acceso a ESXi Shell 123
Establecer el tiempo de espera de disponibilidad o el tiempo de espera de inactividad para ESXi Shell 124
Iniciar sesión en ESXi Shell para solucionar problemas 125
Arranque seguro UEFI para hosts ESXi 125
Ejecutar el script de validación de arranque seguro en un host ESXi actualizado 127
Proteger hosts ESXi con el módulo de plataforma de confianza 128
Ver el estado de atestación de un host ESXi 130
Solucionar problemas de atestación de host ESXi 130
Archivos de registro de ESXi 131
Configurar Syslog en hosts ESXi 131
Ubicaciones de archivos de registro de ESXi 132
Proteger tráfico de registro de Fault Tolerance 133

4 Proteger sistemas vCenter Server 135
Prácticas recomendadas de seguridad de vCenter Server 135
Prácticas recomendadas sobre el control de acceso a vCenter Server 135
Configurar la directiva de contraseñas de vCenter Server 137
Quitar certificados caducados o revocados, y registros de instalaciones con errores 138

Proteger el host de Windows para vCenter Server 138
Limitar la conectividad de red de vCenter Server 139
Evaluación del uso de clientes Linux con CLI y SDK 139
Examinar los complementos del cliente 140
Prácticas recomendadas de seguridad de vCenter Server Appliance 141
Requisitos de contraseñas y comportamiento de bloqueo de vCenter 141
Comprobar huellas digitales para hosts ESXi heredados 143
Puertos necesarios para vCenter Server y Platform Services Controller 143

5 Proteger máquinas virtuales 145
Habilitar o deshabilitar el arranque seguro UEFI para una máquina virtual 145
Limitación de los mensajes informativos de máquinas virtuales a archivos VMX 147
Prácticas recomendadas de seguridad para las máquinas virtuales 148
Protección general de la máquina virtual 148
Usar plantillas para implementar máquinas virtuales 149
Minimizar el uso de la consola de la máquina virtual 150
Evitar que las máquinas virtuales asuman el control de los recursos 150
Deshabilitar funciones innecesarias en máquinas virtuales 151
Quitar dispositivos de hardware innecesarios 152
Deshabilitar las características de visualización que no se utilizan 153
Deshabilitar características no expuestas 153
Impedir que Carpetas compartidas de VMware comparta archivos de host con la máquina virtual 154
Deshabilitar las operaciones para copiar y pegar entre el sistema operativo invitado y la consola remota 155
Limitar la exposición de los datos confidenciales copiados al portapapeles 156
Restringir la ejecución de comandos dentro de una máquina virtual a los usuarios 156
Evitar que un usuario o proceso de máquina virtual desconecten dispositivos 157
Evitar que los procesos del sistema operativo invitado envíen mensajes de configuración al host 158
Evitar utilizar discos independientes no persistentes 158

6 Cifrado de máquinas virtuales 160
Cómo el cifrado de máquinas virtuales de vSphere protege el entorno 161
Componentes de cifrado de máquinas virtuales de vSphere 163
Flujo del proceso de cifrado 165
Cifrado de disco virtual 166
Requisitos previos y privilegios necesarios para tareas de cifrado 167
vSphere vMotion cifrado 169
Interoperabilidad, advertencias y prácticas recomendadas de cifrado 170
Prácticas recomendadas de cifrado de máquinas virtuales 171
Advertencias de cifrado de máquinas virtuales 174

Interoperabilidad del cifrado de máquinas virtuales 175

7 Usar cifrado en el entorno de vSphere 179

Configurar el clúster del servidor de administración de claves 179

Agregar un servidor KMS a vCenter Server en vSphere Client 179

Agregar un servidor KMS a vCenter Server en vSphere Web Client 181

Establecer una conexión de confianza mediante el intercambio de certificados 182

Usar la opción Certificado de CA raíz para establecer una conexión de confianza 183

Usar la opción Certificado para establecer una conexión de confianza 184

Usar la opción Nueva solicitud de firma del certificado para establecer una conexión de confianza 184

Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza 185

Establecer el clúster de KMS predeterminado 186

Completar la instalación de confianza 186

Configurar clústeres de KMS independientes para diferentes usuarios 187

Crear una directiva de almacenamiento de cifrado 188

Habilitar el modo de cifrado de host de forma explícita 189

Deshabilitar el modo de cifrado de host 189

Crear una máquina virtual cifrada 190

Clonar una máquina virtual cifrada 191

Cifrar una máquina virtual o un disco virtual existente 192

Descifrar una máquina virtual o un disco virtual cifrados 194

Cambiar la directiva de cifrado para discos virtuales 195

Resolver problemas de claves faltantes 196

Desbloquear las máquinas virtuales bloqueadas 198

Solucionar problemas del modo de cifrado de host ESXi 199

Volver a habilitar el modo de cifrado de host ESXi 200

Establecer el umbral de caducidad de los certificados del servidor de administración de claves 201

Cifrado de máquinas virtuales de vSphere y volcados de núcleo 201

Recopilar un paquete de vm-support para un host ESXi que usa cifrado 203

Descifrar o volver a cifrar un volcado de núcleo cifrado 204

8 Proteger las máquinas virtuales con el módulo de plataforma de confianza virtual 206

Descripción general del módulo de plataforma de confianza virtual 206

Crear una máquina virtual con un módulo de plataforma de confianza virtual 208

Habilitar el Módulo de plataforma de confianza virtual para una máquina virtual existente 209

Quitar el módulo de plataforma de confianza virtual de una máquina virtual 210

Identificar las máquinas virtuales habilitadas para el módulo de la plataforma de confianza virtual 211

Ver certificados de dispositivo del módulo de plataforma de confianza virtual 212

Exportar y reemplazar certificados de dispositivo del Módulo de plataforma de confianza 212

9 Proteger sistemas operativos invitados Windows con seguridad basada en la virtualización 214

Prácticas recomendadas de seguridad basada en virtualización 215
Habilitar la seguridad basada en virtualización en una máquina virtual 216
Habilitar la seguridad basada en virtualización en una máquina virtual existente 217
Habilitar la seguridad basada en virtualización en el sistema operativo invitado 218
Deshabilitar la seguridad basada en virtualización 219
Identificar máquinas virtuales habilitadas para VBS 219

10 Proteger las redes de vSphere 220

Introducción a la seguridad de red de vSphere 220
Proteger la red con firewalls 222
- Firewalls para configuraciones con vCenter Server 223
- Conexión con vCenter Server mediante un firewall 224
- Conectar hosts ESXi mediante firewalls 224
- Firewalls para configuraciones sin vCenter Server 224
- Conectar con la consola de la máquina virtual mediante un firewall 225

Proteger el conmutador físico 226
Protección de puertos de conmutadores estándar con directivas de seguridad 226
Proteger conmutadores estándar de vSphere 227
- Cambios de dirección MAC 228
- Transmisiones falsificadas 228
- Operación en modo promiscuo 229

Protección de conmutador estándar y VLAN 229
Proteger conmutadores distribuidos y grupos de puertos distribuidos de vSphere 231
Proteger las máquinas virtuales con VLAN 232
- Consideraciones de seguridad para VLAN 233
- Proteger las VLAN 234

Crear varias redes en un único host ESXi 234
Seguridad del protocolo de Internet 237
- Lista de asociaciones de seguridad disponibles 237
- Agregar una asociación de seguridad IPsec 238
- Quitar una asociación de seguridad IPsec 239
- Lista de directivas de seguridad IPsec disponibles 239
- Crear una directiva de seguridad IPsec 239
- Quitar una directiva de seguridad IPsec 240

Garantizar la correcta configuración de SNMP 241
Prácticas recomendadas de seguridad de redes de vSphere 241
- Recomendaciones generales sobre seguridad de redes 242
- Etiquetar componentes de redes 243

Documentación y verificación del entorno VLAN de vSphere 244
Adoptar prácticas de aislamiento de red 245
Usar conmutadores virtuales con vSphere Network Appliance API solo cuando es necesario 246

11 Prácticas recomendadas relacionadas con varios componentes de vSphere 248
Sincronizar los relojes en la red de vSphere 248
Sincronización de los relojes de ESXi con un servidor horario de red 249
Configurar la sincronización de hora en vCenter Server Appliance 250
Usar la sincronización de hora de VMware Tools 250
Agregar o reemplazar servidores NTP en la configuración de vCenter Server Appliance 251
Sincronizar la hora de vCenter Server Appliance con un servidor NTP 252
Prácticas recomendadas de seguridad de almacenamiento 253
Proteger almacenamiento iSCSI 253
Proteger dispositivos de iSCSI 253
Proteger una SAN iSCSI 254
Crear máscaras y dividir en zonas para recursos de SAN 255
Usar Kerberos para NFS 4.1 255
Comprobar que está deshabilitado el envío de datos de rendimiento del host a los invitados 257
Configurar tiempos de espera de ESXi Shell y vSphere Web Client 257

12 Administración de la configuración del protocolo TLS con la utilidad de configuración de TLS 259
Puertos que permiten deshabilitar versiones de TLS 260
Habilitar o deshabilitar versiones de TLS en vSphere 261
Copia de seguridad manual opcional 261
Habilitar o deshabilitar versiones de TLS en sistemas de vCenter Server 263
Habilitar o deshabilitar versiones de TLS en hosts ESXi 264
Habilitar o deshabilitar versiones de TLS en sistemas Platform Services Controller externos 266
Buscar protocolos TLS habilitados en vCenter Server 267
Revertir los cambios de configuración de TLS 268
Habilitar o deshabilitar las versiones de TLS en vSphere Update Manager en Windows 270
Deshabilitar las versiones anteriores de TLS para Update Manager, puerto 9087 270
Deshabilitar las versiones anteriores de TLS para Update Manager, puerto 8084 271
Volver a habilitar las versiones de TLS deshabilitadas para el puerto 9087 de Update Manager 273
Volver a habilitar las versiones de TLS deshabilitadas para el puerto 8084 de Update Manager 273

13 Privilegios definidos 275
Privilegios de alarmas 276

Privilegios de Auto Deploy y perfiles de imagen 277
Privilegios de los certificados 278
Privilegios de la biblioteca de contenido 278
Privilegios de operaciones de cifrado 281
Privilegios de centro de datos 283
Privilegios de almacenes de datos 284
Privilegios de clústeres de almacenes de datos 285
Privilegios de Distributed Switch 285
Privilegios de ESX Agent Manager 286
Privilegios de extensiones 287
Privilegios de proveedor de estadísticas externos 287
Privilegios de carpeta 287
Privilegios globales 288
Privilegios de proveedor de actualización de estado 289
Privilegios de CIM para hosts 289
Privilegios de configuración de hosts 290
Inventario del host 291
Privilegios de operaciones locales en hosts 292
Privilegios de vSphere Replication de host 293
Privilegios de perfiles de host 293
Privilegios de red 293
Privilegios de rendimiento 294
Privilegios de permisos 294
Privilegios de almacenamiento basado en perfiles 295
Privilegios de recursos 295
Privilegios para tareas programadas 296
Privilegios de sesiones 297
Privilegios de vistas de almacenamiento 297
Privilegios de tareas 298
Privilegios del servicio de transferencia 298
Privilegios de configuración de máquinas virtuales 298
Privilegios de operaciones de invitado de máquina virtual 301
Privilegios para la interacción con máquinas virtuales 302
Privilegios de inventario de máquinas virtuales 305
Privilegios de aprovisionamiento de las máquinas virtuales 306
Privilegios de configuración de servicios de la máquina virtual 307
Privilegios de administración de snapshots de las máquinas virtuales 308
Privilegios de vSphere Replication de máquinas virtuales 309
Privilegios de grupo dvPort 309
Privilegios de vApp 310
Privilegios de vServices 311

Privilegios de etiquetado de vSphere 312

14 Descripción general de fortalecimiento y cumplimiento de vSphere 314

Seguridad y conformidad en el entorno de vSphere 314

Descripción general de la guía de configuración de seguridad de vSphere 317

Acerca del Instituto nacional de estándares y tecnología 320

Acerca de STIG de DISA 321

Acerca del ciclo de vida de desarrollo de seguridad de VMware 321

Registro de auditoría 322

Eventos de auditoría de Single Sign-On 322

Descripción general de los próximos pasos de seguridad y conformidad 324

Acerca de la seguridad de vSphere

Seguridad de vSphere proporciona información sobre cómo proteger el entorno de vSphere® para VMware® vCenter® Server y VMware ESXi.

A modo de ayuda para proteger el entorno de vSphere, en esta documentación se describen las características de seguridad disponibles y las medidas que se pueden adoptar para proteger el entorno contra ataques.

Tabla 1-1. Información destacada de *Seguridad de vSphere*

Temas	Contenido destacado
Administración de usuarios y permisos	■ Modelo de permisos (funciones, grupos y objetos). ■ Crear funciones personalizadas. ■ Crear permisos. ■ Administrar permisos globales.
Características de seguridad del host	■ Modo de bloqueo y otras funciones del perfil de seguridad ■ Autenticación de la tarjeta inteligente del host ■ vSphere Authentication Proxy ■ Arranque seguro UEFI ■ Módulo de plataforma de confianza (Trusted Platform Module, TPM)
Cifrado de máquinas virtuales	■ Funcionamiento del cifrado de máquinas virtuales ■ Configuración de KMS ■ Cifrado y descifrado de máquinas virtuales ■ Solución de problemas y prácticas recomendadas
Seguridad del sistema operativo invitado	■ Módulo de plataforma de confianza virtual (Virtual Trusted Platform Module, vTPM) ■ Seguridad basada en virtualización (Virtualization Based Security, VBS)
Administrar la configuración del protocolo TLS	Cambio de la configuración del protocolo TLS mediante una utilidad de línea de comandos.
Prácticas recomendadas y fortalecimiento de la seguridad	Prácticas recomendadas y consejos de expertos en seguridad de VMware. ■ Seguridad de vCenter Server ■ Seguridad de los hosts ■ Seguridad de las máquinas virtuales ■ Seguridad de las redes
Privilegios de vSphere	Lista completa de todos los privilegios de vSphere admitidos en esta versión.

Documentación relacionada

En el documento complementario *Administrar Platform Services Controller*, se explica cómo se pueden utilizar los servicios de Platform Services Controller, por ejemplo, para administrar la autenticación con vCenter Single Sign-On, así como los certificados en el entorno de vSphere.

Además de estos documentos, VMware publica la *guía de configuración de seguridad de vSphere* (anteriormente denominada la *Guía de fortalecimiento*) para cada versión de vSphere. Puede obtener dicha guía en http://www.vmware.com/security/hardening-guides.html. La *guía de configuración de seguridad de vSphere* contiene directrices de configuración de seguridad que el cliente puede o debe definir, así como la configuración de seguridad proporcionada por VMware que el cliente debe auditar para garantizar que aún tiene el valor predeterminado.

Audiencia prevista

Esta información está dirigida a administradores de sistemas Windows y Linux expertos que están familiarizados con la tecnología de máquina virtual y las operaciones de centro de datos.

vSphere Client y vSphere Web Client

Las instrucciones de esta guía reflejan vSphere Client (GUI basada en HTML5). También puede utilizar las instrucciones para realizar las tareas mediante vSphere Web Client (GUI basada en Flex).

Las tareas para las que el flujo de trabajo difiere significativamente entre vSphere Client y vSphere Web Client tienen procedimientos duplicados que proporcionan los pasos de acuerdo con la interfaz del cliente correspondiente. Los procedimientos que se relacionan con vSphere Web Client, contienen vSphere Web Client en el título.

Nota En vSphere 6.7 Update 1, casi todas las funcionalidades de vSphere Web Client se implementan en vSphere Client. Para obtener una lista actualizada del resto de las funcionalidades no compatibles, consulte Actualizaciones de funcionalidades para vSphere Client.

Certificaciones

VMware difunde una lista pública de productos de VMware que hayan completado certificaciones de criterios comunes. Para comprobar si se certificó una versión de un producto de VMware en particular, consulte la página web de evaluación y validación de criterios comunes: https://www.vmware.com/security/certifications/common-criteria.html.

Compatibilidad con el estándar federal de procesamiento de la información 140-2

A partir de la versión 6.7, vCenter Server admite el estándar federal de procesamiento de la información (Federal Information Processing Standard, FIPS) 140-2.

FIPS 140-2 es un estándar del gobierno de EE. UU. y Canadá que especifica los requisitos de seguridad para módulos criptográficos. De forma predeterminada, FIPS 140-2 siempre está habilitado después de la instalación o la actualización de vCenter Server 6.7 o posterior, y de ESXi 6.7 o posterior.

Para obtener más información sobre la compatibilidad con FIPS 140-2 en productos de VMware, consulte https://www.vmware.com/security/certifications/fips.html.

Información actualizada

Este documento sobre *Seguridad de vSphere* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de la documentación sobre *Seguridad de vSphere*.

Revisión	Descripción
28 de abril de 2022	■ Actualización menor a Privilegios de vistas de almacenamiento.
21 MAR 2022	■ Se corrigió un error ortográfico en Cargar una clave SSH mediante un comando vifs. ■ Actualización menor a Certificados y actualizaciones de hosts. ■ Se solucionaron comandos incorrectos en el paso 4 de Usar certificados personalizados con Auto Deploy. ■ Actualización menor a Restaurar archivos de certificados y claves de ESXi. ■ Se eliminó la información tabular de Puertos de firewall entrantes y salientes para hosts de ESXi, Puertos necesarios para vCenter Server y Platform Services Controller y Puertos que permiten deshabilitar versiones de TLS. En adelante, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/. Como parte de la transición de toda la información de los puertos a la herramienta Ports and Protocols, también se ha eliminado el tema sobre puertos TCP y UDP adicionales de vCenter Server. ■ Se agregó información a Interoperabilidad del cifrado de máquinas virtuales. ■ Actualización menor a Solucionar problemas del modo de cifrado de host ESXi. ■ Se agregaron los privilegios necesarios a Crear una máquina virtual con un módulo de plataforma de confianza virtual, Habilitar el Módulo de plataforma de confianza virtual para una máquina virtual existente y Quitar el módulo de plataforma de confianza virtual de una máquina virtual. ■ Para un host ESXi independiente, se aclaró que debe ejecutar el comando `reconfigureEsx ESXiHost` desde un sistema vCenter Server en Habilitar o deshabilitar versiones de TLS en hosts ESXi.
22 de octubre de 2021	■ Se actualizaron Reemplazo de la clave y el certificado predeterminados con el comando vifs y Reemplazar un certificado predeterminado mediante el método PUT de HTTPS con una alternativa para reiniciar los agentes de administración después de reemplazar el certificado. ■ Actualización menor a Usar vSphere Authentication Proxy para agregar un host a un dominio. ■ Se corrigió un error tipográfico en Cambiar la directiva de cifrado para discos virtuales. ■ Se corrigió un comando en Garantizar la correcta configuración de SNMP. ■ Actualización menor a Revertir los cambios de configuración de TLS. ■ Actualización menor a Acerca de STIG de DISA. ■ Actualización menor a Eventos de auditoría de Single Sign-On.

Revisión	Descripción
31 de marzo de 2021	■ Actualización menor a Recursos y prácticas recomendadas de seguridad. ■ Se actualizaron varios temas en Capítulo 2 Tareas de administración de permisos y usuarios de vSphere. ■ Actualización menor a Capítulo 3 Proteger hosts ESXi. ■ Se actualizó Bloqueo de cuenta y contraseñas ESXi para incluir más información sobre las opciones de contraseña. ■ Actualización menor a Seguridad de SSH. ■ Actualización menor a Recomendaciones de seguridad para redes de ESXi. ■ Actualización menor a Ver la información de caducidad de certificados de varios hosts ESXi. ■ Se actualizó Renovar o actualizar de certificados de ESXi para incluir los pasos de verificación. ■ Se actualizó Requisitos de las solicitudes de firma de certificados de ESXi con más información sobre la generación de las CSR. ■ Se actualizó Administrar los niveles de aceptación de hosts y VIB para corregir la sintaxis del comando de la CLI y para aclarar dónde se debe dar soporte a los VIB VMwareAccepted y PartnerSupported. ■ Se actualizó Crear un tiempo de espera para sesiones de ESXi Shell inactivas para mostrar que un valor de cero (0) deshabilita el tiempo de inactividad. ■ Actualización menor a Usar la interfaz de usuario de la consola directa para habilitar el acceso a ESXi Shell. ■ Actualización menor a Proteger hosts ESXi con el módulo de plataforma de confianza. ■ Se actualizó Solucionar problemas de atestación de host ESXi para agregar más información sobre la comprobación del archivo `vpxd.log`. ■ Actualización menor a Capítulo 5 Proteger máquinas virtuales. ■ Actualización menor a Minimizar el uso de la consola de la máquina virtual. ■ Actualización menor a Evitar que las máquinas virtuales asuman el control de los recursos. ■ Actualización menor a Deshabilitar funciones innecesarias en máquinas virtuales. ■ Se actualizó Deshabilitar las características de visualización que no se utilizan para mostrar que necesita apagar la máquina virtual. ■ Se actualizaron varios temas en Capítulo 8 Proteger las máquinas virtuales con el módulo de plataforma de confianza virtual. ■ Se actualizó Recomendaciones generales sobre seguridad de redes con más información sobre el protocolo de árbol de expansión (Spanning Tree Protocol, STP). ■ Se actualizó Adoptar prácticas de aislamiento de red con información sobre el aislamiento del tráfico de vSAN. ■ Se actualizaron varios temas en Capítulo 14 Descripción general de fortalecimiento y cumplimiento de vSphere.
13 de agosto de 2020	En VMware, valoramos la inclusión. Para fomentar este principio entre nuestros clientes, nuestros partners y nuestra comunidad interna, estamos reemplazando parte de la terminología en nuestro contenido. Hemos actualizado esta guía para eliminar el lenguaje no inclusivo.
18 de junio de 2020	■ Se actualizó Privilegios necesarios para la realización de tareas comunes para mostrar los privilegios necesarios para agregar un único host a un centro de datos y agregar varios hosts al clúster. ■ Se actualizó Reemplazo de certificados y claves SSL de ESXi con un vínculo al artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/56441 (Configurar certificados personalizados en ESXi hosts para autenticar hosts vSAN). ■ Se agregó el puerto 15080 (puerto interno del servicio de análisis) a la información de los puertos. ■ Actualización menor a Quitar el módulo de plataforma de confianza virtual de una máquina virtual.

Revisión	Descripción
28 de abril de 2020	■ Se actualizó el Reemplazo de certificados y claves SSL de ESXi para consultar la información correcta sobre el uso de certificados personalizados. ■ Actualización menor a Evitar que un usuario o proceso de máquina virtual desconecten dispositivos. ■ Se actualizaron los privilegios necesarios para mover los hosts a un clúster en Privilegios necesarios para la realización de tareas comunes. ■ Se agregó información sobre la versión 11.0 de VMware Remote Console a Conectar con la consola de la máquina virtual mediante un firewall. ■ Se eliminó la referencia cruzada para "Habilitar o deshabilitar un servicio" en Habilitar vSphere Authentication Proxy, ya que no se aplica a vCenter Server. ■ Actualización menor a Usar la interfaz de usuario de la consola directa para habilitar el acceso a ESXi Shell. ■ Se actualizaron los videos de Agregar direcciones IP permitidas para un host ESXi y Configurar firewalls de ESXi para mostrar el vSphere Client. ■ Se agregó una referencia a la documentación de *Redes de vSphere* sobre la configuración de adaptadores de máquinas virtuales para el modo promiscuo en Operación en modo promiscuo. ■ Configuración predeterminada de certificados ESXi ahora muestra el parámetro correcto para "Número de días que el certificado es válido" (vpxd.certmgmt.certs.daysValid).
23 de diciembre de 2019	■ Se corrigió la información sobre el puerto 80 y el puerto 9000 para mostrar que son conexiones de Firewall salientes en Puertos de firewall entrantes y salientes para hosts de ESXi. ■ Se corrigió un vínculo en Acerca de STIG de DISA.
14 de noviembre 2019	■ Se agregó información sobre la compatibilidad de vSphere para el estándar federal de procesamiento de información 140-2 en Acerca de la seguridad de vSphere. ■ Se agregó el nombre de archivo y la ubicación del registro para Quick Boot a Ubicaciones de archivos de registro de ESXi. ■ Se corrigió la información sobre el puerto 9080 para mostrar que es una conexión de Firewall entrante en Puertos de firewall entrantes y salientes para hosts de ESXi.
27 de agosto de 2019	■ Se corrigieron pasos en Sincronización de los relojes de ESXi con un servidor horario de red. ■ Se realizó una actualización menor a Privilegios de configuración de servicios de la máquina virtual.
10 de julio de 2019	■ Se actualizaron Prácticas recomendadas de seguridad basada en virtualización, Habilitar la seguridad basada en virtualización en una máquina virtual y Habilitar la seguridad basada en virtualización en una máquina virtual existente para reflejar que la seguridad basada en virtualización (Virtualization-Based Security, VBS) ahora es compatible con Microsoft Server 2019. ■ Se realizaron actualizaciones menores para Interoperabilidad del cifrado de máquinas virtuales y vSphere vMotion cifrado.
11 de abril de 2019	Versión inicial.

Seguridad en el entorno de vSphere

1

Los componentes de un entorno de vSphere vienen protegidos desde el inicio mediante varias características, como autenticación, autorización, un firewall en cada host ESXi, etc. La configuración predeterminada se puede modificar de varias maneras. Por ejemplo, se pueden establecer permisos en los objetos de vCenter, abrir puertos de firewall o cambiar los certificados predeterminados. Es posible tomar medidas de seguridad para diferentes objetos en la jerarquía de objetos de vCenter, por ejemplo, sistemas vCenter Server, hosts ESXi, máquinas virtuales, y objetos de redes y de almacenamiento.

La descripción general detallada de las diferentes áreas de vSphere que requieren atención permite planificar la estrategia de seguridad. También se pueden aprovechar otros recursos de seguridad de vSphere disponibles en el sitio web de VMware.

Este capítulo incluye los siguientes temas:

- Proteger hipervisor de ESXi
- Proteger los sistemas vCenter Server y los servicios asociados
- Proteger máquinas virtuales
- Proteger la capa de redes virtuales
- Contraseñas en el entorno de vSphere
- Recursos y prácticas recomendadas de seguridad

Proteger hipervisor de ESXi

El hipervisor de ESXi ya viene protegido. Puede aumentar la protección de los hosts ESXi con el modo de bloqueo y otras características integradas. A los fines de coherencia, puede configurar un host de referencia y mantener todos los hosts sincronizados con el perfil de host del host de referencia. También puede proteger el entorno con la administración generada por script para garantizar que los cambios se apliquen a todos los hosts.

Puede mejorar la protección de los hosts ESXi administrados por vCenter Server mediante las siguientes acciones. Consulte el informe técnico *Seguridad de VMware vSphere Hypervisor* para conocer el contexto y obtener más información.

Limitar el acceso a ESXi

De forma predeterminada, los servicios de ESXi Shell y SSH no se ejecutan, y solo el usuario raíz puede iniciar sesión en la interfaz de usuario de la consola directa (DCUI). Si decide habilitar el acceso a ESXi o SSH, puede establecer los tiempos de espera para reducir el riesgo de que se produzca un acceso no autorizado.

Los usuarios que pueden acceder al host ESXi deben tener permisos para administrar el host. Puede establecer permisos en el objeto de host del sistema vCenter Server que administra el host.

Utilizar usuarios designados y privilegio mínimo

De manera predeterminada, el usuario raíz puede realizar muchas tareas. No permita que los administradores inicien sesión en el host ESXi con la cuenta de usuario raíz. En su lugar, cree usuarios administradores designados de vCenter Server y asigne la función de administrador a dichos usuarios. También puede asignar una función personalizada a esos usuarios. Consulte Crear una función personalizada.

Si administra usuarios directamente en el host, las opciones de administración de funciones son limitadas. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*.

Reducir la cantidad de puertos de firewall de ESXi abiertos

De forma predeterminada, los puertos de firewall del host ESXi se abren solo cuando se inicia el servicio correspondiente. Se pueden utilizar los comandos de vSphere Client, ESXCLI o PowerCLI para comprobar y administrar el estado de los puertos de firewall.

Consulte Configurar firewalls de ESXi.

Automatizar la administración de hosts ESXi

Ya que generalmente es importante que diferentes hosts del mismo centro de datos estén sincronizados, utilice la instalación generada por script o vSphere Auto Deploy para aprovisionar los hosts. Los hosts se pueden administrar con los scripts. Los perfiles de host son una alternativa a la administración generada por script. Se debe configurar un host de referencia, exportar el perfil de host y aplicar el perfil de host a todos los hosts. El perfil de host se puede aplicar directamente o como parte del aprovisionamiento con Auto Deploy.

Consulte Usar scripts para administrar las opciones de configuración de hosts y la documentación *Instalar y configurar vCenter Server* para obtener información sobre vSphere Auto Deploy.

Aprovechar el modo de bloqueo

En el modo de bloqueo, solo se puede acceder a los hosts ESXi a través de vCenter Server de forma predeterminada. A partir de vSphere 6.0, es posible seleccionar el modo de bloqueo estricto o el modo de bloqueo normal. Puede definir los usuarios con excepción para permitir el acceso directo a las cuentas de servicio, como agentes de copias de seguridad.

Consulte Modo de bloqueo.

Comprobar la integridad de los paquetes de VIB

Cada paquete de VIB tiene un nivel de aceptación asociado. Es posible agregar un VIB a un host ESXi solo si el nivel de aceptación de VIB es el mismo o mejor que el nivel de aceptación del host. No se puede agregar un VIB CommunitySupported o PartnerSupported a un host a menos que se cambie de forma explícita el nivel de aceptación del host.

Consulte Administrar los niveles de aceptación de hosts y VIB.

Administrar certificados de ESXi

En vSphere 6.0 y versiones posteriores, VMware Certificate Authority (VMCA) aprovisiona cada host ESXi con un certificado firmado cuya entidad de certificación raíz de forma predeterminada es VMCA. Si las directivas de la empresa lo requieren, puede reemplazar los certificados existentes con certificados firmados por una CA empresarial o de terceros.

Consulte Administrar certificados para hosts ESXi.

Consideración de la autenticación de tarjeta inteligente

A partir de vSphere 6.0, ESXi admite el uso de autenticación de tarjeta inteligente en lugar de la autenticación de nombre de usuario y contraseña. Para mayor seguridad, puede configurar la autenticación de tarjeta inteligente. También se admite la autenticación en dos fases para vCenter Server. Puede configurar al mismo tiempo la autenticación con nombre de usuario y contraseña, y la autenticación de tarjeta inteligente.

Consulte Configurar la autenticación de tarjeta inteligente de ESXi.

Consideración de bloqueo de cuentas de ESXi

A partir de vSphere 6.0, se admite el bloqueo de cuentas para el acceso a través de SSH y vSphere Web Services SDK. De forma predeterminada, se permite un máximo de 10 intentos con errores antes de que la cuenta se bloquee. De forma predeterminada, la cuenta se desbloquea después de dos minutos.

Nota La interfaz de la consola directa (DCUI) y ESXi Shell no admiten el bloqueo de cuentas.

Consulte Bloqueo de cuenta y contraseñas ESXi.

Los parámetros de seguridad de los hosts individuales son similares, pero las tareas de administración pueden ser diferentes. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*.

Proteger los sistemas vCenter Server y los servicios asociados

El sistema vCenter Server y los servicios asociados están protegidos por autenticación mediante vCenter Single Sign-On y por autorización mediante el modelo de permisos de vCenter Server. Es posible modificar el comportamiento predeterminado y seguir los pasos adicionales para limitar el acceso al entorno.

Cuando proteja el entorno de vSphere, tenga en cuenta que se deben proteger todos los servicios que están asociados con las instancias de vCenter Server. En ciertos entornos, se pueden proteger varias instancias de vCenter Server y una o más instancias de Platform Services Controller.

Fortalecer todos los equipos host de vCenter

El primer paso para proteger el entorno de vCenter es fortalecer cada equipo en el que se ejecutan vCenter Server o un servicio asociado. El enfoque es similar cuando se trata de una máquina física o una máquina virtual. Siempre instale las revisiones de seguridad más recientes para el sistema operativo y siga las prácticas recomendadas estándar de la industria para proteger el equipo host.

Obtener información sobre el modelo de certificado de vCenter

De forma predeterminada, VMware Certificate Authority aprovisiona cada host ESXi, cada máquina del entorno y cada usuario de solución con un certificado firmado por VMCA. El entorno se pone en funcionamiento desde el comienzo, pero si la empresa lo requiere, se puede cambiar el comportamiento predeterminado. Consulte la documentación de *Administrar Platform Services Controller* para obtener detalles.

Para mejorar la protección, quite explícitamente los certificados caducados o revocados y las instalaciones con errores.

Configuración de vCenter Single Sign-On

vCenter Server y los servicios asociados están protegidos con el marco de autenticación de vCenter Single Sign-On. Cuando instale el software por primera vez, especifique una contraseña para el administrador del dominio de vCenter Single Sign-On, administrator@vsphere.local de manera predeterminada. Solo ese dominio está inicialmente disponible como un origen de identidad. Es posible agregar otros orígenes de identidad, ya sea de Active Directory o LDAP, y establecer un origen de identidad predeterminado. Posteriormente, los usuarios que se pueden autenticar en uno de esos orígenes de identidad pueden ver objetos y realizar tareas si tienen la autorización para hacerlo. Consulte la documentación de *Administrar Platform Services Controller* para obtener detalles.

Asignar funciones a usuarios o grupos designados

Para mejorar el registro, asocie los permisos que otorga a un objeto con un usuario o grupo designado, y una función predefinida o personalizada. El modelo de permisos de vSphere 6.0 es muy flexible porque ofrece varios modos de autorizar usuarios o grupos. Consulte Descripción de la autorización en vSphere y Privilegios necesarios para la realización de tareas comunes.

Restrinja los privilegios de administrador y el uso de la función de administrador. De ser posible, no utilice el usuario administrador anónimo.

Configurar NTP

Configure el NTP para cada nodo del entorno. La infraestructura de certificados requiere una marca de tiempo precisa y no funciona correctamente si los nodos no están sincronizados.

Consulte Sincronizar los relojes en la red de vSphere.

Proteger máquinas virtuales

Para proteger las máquinas virtuales, mantenga revisados los sistemas operativos invitados y proteja el entorno como si fuera una máquina física. Considere deshabilitar las funcionalidades innecesarias, minimizar el uso de la consola de la máquina virtual y cumplir con las prácticas recomendadas.

Proteger el sistema operativo invitado

Para proteger el sistema operativo invitado, asegúrese de utilizar las revisiones más recientes y, si corresponde, las aplicaciones antispyware y antimalware. Consulte la documentación del proveedor del sistema operativo invitado. También puede consultar otra información disponible en libros o en Internet para el sistema operativo.

Deshabilitar funcionalidades innecesarias

Compruebe que las funcionalidades innecesarias estén deshabilitadas para minimizar los puntos de ataque potenciales. Muchas de las características que no se usan con frecuencia se deshabilitan de manera predeterminada. Quite el hardware que no necesite y deshabilite ciertas funciones, como Host-Guest Filesystem (HGFS), o bien copie y pegue entre la máquina virtual y una consola remota.

Consulte Deshabilitar funciones innecesarias en máquinas virtuales.

Utilizar plantillas y la administración generada por script

Las plantillas de máquina virtual permiten configurar el sistema operativo de modo que cumpla con sus requisitos y crear otras máquinas virtuales con la misma configuración.

Si quiere cambiar la configuración de la máquina virtual después de la implementación inicial, considere usar scripts, por ejemplo, PowerCLI. En esta documentación, se explica cómo realizar tareas mediante la GUI. Considere usar scripts en lugar de la GUI para mantener la coherencia de su entorno. En los entornos de gran tamaño, puede agrupar las máquinas virtuales en carpetas para optimizar el proceso de scripting.

Para obtener información sobre plantillas, consulte Usar plantillas para implementar máquinas virtuales y *Administrar máquinas virtuales de vSphere*. Para obtener información sobre PowerCLI, consulte la documentación de VMware PowerCLI.

Minimizar el uso de la consola de la máquina virtual

La consola de máquina virtual cumple la misma función en la máquina virtual que el monitor de un servidor físico. Los usuarios que tienen acceso a una consola de máquina virtual pueden acceder a la gestión de energía de la máquina virtual y a controles de conectividad del dispositivo extraíble. Como resultado, el acceso a la consola de máquina virtual puede permitir un ataque malicioso en la máquina virtual.

Considerar el arranque seguro UEFI

A partir de vSphere 6.5, puede configurar la máquina virtual para usar el arranque UEFI. Si el sistema operativo admite el arranque seguro UEFI, puede seleccionar la opción para las máquinas virtuales a fin de aumentar la seguridad. Consulte Habilitar o deshabilitar el arranque seguro UEFI para una máquina virtual.

Considere el uso de VMware AppDefense

A partir de vSphere 6.7 Update 1, puede instalar y utilizar el complemento VMware AppDefense para proteger las aplicaciones y garantizar la seguridad del endpoint. El complemento AppDefense está disponible con la licencia Platinum de vSphere. Si tiene la licencia Platinum, el panel AppDefense aparece en la pestaña **Resumen** de cualquier máquina virtual en el inventario. Desde ese panel, puede instalar, actualizar o ver los detalles sobre el complemento AppDefense. Para obtener más información sobre VMware AppDefense, consulte la documentación de *AppDefense*.

Proteger la capa de redes virtuales

La capa de redes virtuales incluye adaptadores de red virtual, conmutadores virtuales, conmutadores virtuales distribuidos, y puertos y grupos de puertos. ESXi se basa en la capa de redes virtuales para establecer las comunicaciones entre las máquinas virtuales y sus usuarios. Asimismo, ESXi utiliza la capa de redes virtuales para comunicarse con SAN iSCSI, el almacenamiento NAS, etc.

vSphere incluye la matriz completa de características necesarias para una infraestructura segura de redes. Puede proteger cada elemento de la infraestructura por separado, como los conmutadores virtuales, los conmutadores virtuales distribuidos y los adaptadores de red virtuales. Por otra parte, considere las siguientes instrucciones, que se analizan más detalladamente en Capítulo 10 Proteger las redes de vSphere.

Aislar el tráfico de red

El aislamiento del tráfico de red es fundamental para proteger el entorno de ESXi. Las distintas redes requieren distintos niveles de aislamiento y acceso. La red de administración aísla los distintos tráficos (tráfico de clientes, de la interfaz de la línea de comandos [Command-Line Interface, CLI] o de la API y del software de terceros) del tráfico normal. Asegúrese de que solo los administradores de sistemas, redes y seguridad puedan acceder a la red de administración.

Consulte Recomendaciones de seguridad para redes de ESXi.

Utilizar firewalls para proteger los elementos de la red virtual

Puede abrir y cerrar los puertos de firewall y proteger cada elemento de la red virtual por separado. Para los hosts ESXi, las reglas de firewall asocian los servicios con los firewalls correspondientes, y pueden abrir y cerrar el firewall de acuerdo con el estado del servicio.

También es posible abrir puertos en instancias de Platform Services Controller y vCenter Server de forma explícita.

Para obtener la lista de todos los puertos y protocolos compatibles en los productos de VMware, incluidos vSphere y vSAN, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/. Puede buscar puertos por producto de VMware, crear una lista de puertos personalizada e imprimir o guardar listas de puertos.

Considerar las directivas de seguridad de redes

Las directivas de seguridad de redes ayudan a proteger el tráfico contra la suplantación de direcciones MAC y la exploración de puertos no deseada. La directiva de seguridad de un conmutador estándar o distribuido se implementa en la Capa 2 (capa de vínculo de datos) de la pila del protocolo de red. Los tres elementos de la directiva de seguridad son el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas.

Consulte la documentación de *Redes de vSphere* para ver las instrucciones.

Protección de redes de máquinas virtuales

Los métodos que se utilizan para proteger las redes de máquinas virtuales dependen de varios factores, entre otros:

- El sistema operativo invitado que está instalado.
- Si las máquinas virtuales operan en un entorno de confianza.

Los conmutadores virtuales y los conmutadores virtuales distribuidos proporcionan una protección significativa cuando se utilizan junto con otras prácticas de seguridad comunes, como la instalación de firewalls.

Consulte Capítulo 10 Proteger las redes de vSphere.

Considerar VLAN para proteger el entorno

ESXi es compatible con VLAN de IEEE 802.1q. Las redes VLAN permiten segmentar una red física. Puede utilizar las VLAN para proteger aún más la configuración de la red o el almacenamiento de las máquinas virtuales. Cuando se utilizan redes VLAN, dos máquinas virtuales de la misma red física no pueden enviar ni recibir paquetes entre ellas a menos que se encuentren en la misma VLAN.

Consulte Proteger las máquinas virtuales con VLAN.

Proteger las conexiones con el almacenamiento virtualizado

Una máquina virtual almacena archivos del sistema operativo, archivos de programas y otros datos en un disco virtual. Cada disco virtual figura en la máquina virtual como una unidad SCSI que está conectada a una controladora SCSI. La máquina virtual está aislada de los detalles de almacenamiento y no puede acceder a la información del LUN donde reside el disco virtual.

Virtual Machine File System (VMFS) es un sistema de archivos distribuidos y un administrador de volúmenes que presenta volúmenes virtuales en el host ESXi. Usted es responsable de proteger la conexión con el almacenamiento. Por ejemplo, si utiliza el almacenamiento iSCSI, puede configurar el entorno para usar CHAP. Si la directiva de la empresa lo requiere, puede configurar CHAP mutuo. Utilice vSphere Client o la CLI para configurar CHAP.

Consulte Prácticas recomendadas de seguridad de almacenamiento.

Evaluar la utilización de IPsec

ESXi admite IPsec para IPv6. No se puede utilizar IPsec para IPv4.

Consulte Seguridad del protocolo de Internet.

Contraseñas en el entorno de vSphere

La restricción y la caducidad de las contraseñas y el bloqueo de cuentas en el entorno de vSphere dependen de qué sistema el usuario utiliza como destino, quién es el usuario y cómo se establecen las directivas.

Contraseñas de ESXi

Las restricciones de contraseñas de ESXi se determinan en el módulo PAM de Linux `pam_passwdqc`. Consulte `pam_passwdqc` en la página del manual de Linux y vea Bloqueo de cuenta y contraseñas ESXi.

Contraseñas de vCenter Server y otros servicios de vCenter

vCenter Single Sign-On administra la autenticación de todos los usuarios que inician sesión en vCenter Server y en otros servicios de vCenter. La restricción y la caducidad de las contraseñas y el bloqueo de cuentas dependen de cuál es el dominio del usuario y quién es el usuario.

Administrador de vCenter Single Sign-On

La contraseña para el usuario administrator@vsphere.local, o el usuario administrator@*mydomain* si se seleccionó un dominio distinto durante la instalación, no caduca y no está sujeta a la directiva de bloqueo. En los demás casos, la contraseña debe cumplir con las restricciones establecidas en la directiva de contraseñas de vCenter Single Sign-On. Consulte *Administrar Platform Services Controller* para obtener detalles.

Si olvida la contraseña de este usuario, busque información en la base de conocimientos de VMware sobre la forma de restablecer esta contraseña. El restablecimiento requiere privilegios adicionales, como el acceso raíz al sistema vCenter Server.

Otros usuarios del dominio vCenter Single Sign-On

Las contraseñas de otros usuarios de vsphere.local o de los usuarios del dominio que se especificó durante la instalación deben cumplir con las restricciones establecidas en la directivas de bloqueo y de contraseñas de vCenter Single Sign-On. Consulte *Administrar Platform Services Controller* para obtener detalles. Estas contraseñas caducan de manera predeterminada a los 90 días. Los administradores pueden cambiar la fecha de caducidad como parte de la directiva de contraseñas.

Si olvida la contraseña de vsphere.local, un usuario administrador puede restablecerla mediante el comando `dir-cli`.

Otros usuarios

La restricción y la caducidad de las contraseñas y el bloqueo de cuentas de todos los demás usuarios se determinan según el dominio (el origen de identidad) en el cual el usuario puede autenticarse.

vCenter Single Sign-On admite un origen de identidad predeterminado. Los usuarios pueden iniciar sesión en el dominio correspondiente mediante vSphere Client solo con sus nombres de usuario. Si los usuarios desean iniciar sesión en un dominio no predeterminado, pueden incluir el nombre del dominio, es decir, especificar *user@domain* o *domain**user*. Los parámetros para la contraseña del dominio se aplican a todos los dominios.

Contraseñas de los usuarios de la interfaz de usuario de la consola directa de vCenter Server Appliance

vCenter Server Appliance es una máquina virtual preconfigurada basada en Linux, que está optimizada para ejecutar vCenter Server y los servicios asociados en Linux.

Estas contraseñas se especifican durante la implementación de vCenter Server Appliance.

- Contraseña del usuario raíz del sistema operativo Linux del dispositivo.
- Contraseña predeterminada para el administrador del dominio de vCenter Single Sign-On, administrator@vsphere.local.

Es posible cambiar la contraseña del usuario raíz y realizar otras tareas de administración de usuarios locales de vCenter Server Appliance desde la consola del dispositivo. Consulte *Configuración de vCenter Server*.

Recursos y prácticas recomendadas de seguridad

Si sigue las prácticas recomendadas, ESXi y vCenter Server pueden alcanzar el mismo nivel de seguridad, o incluso uno mayor, que un entorno donde no existe la virtualización.

En este manual se incluyen las prácticas recomendadas para los distintos componentes de la infraestructura de vSphere.

Tabla 1-1. Prácticas recomendadas de seguridad

Componente de vSphere	Recurso
Host ESXi	Capítulo 3 Proteger hosts ESXi
Sistema vCenter Server	Prácticas recomendadas de seguridad de vCenter Server
Máquina virtual	Prácticas recomendadas de seguridad para las máquinas virtuales
Redes de vSphere	Prácticas recomendadas de seguridad de redes de vSphere

Este manual es tan solo una de las fuentes que debe emplear para garantizar un entorno seguro.

Los recursos de seguridad de VMware, incluidas alertas y descargas, se encuentran disponibles en la Web.

Tabla 1-2. Recursos de seguridad de VMware en la Web

Tema	Recurso
Información sobre seguridad y operaciones de ESXi y vCenter Server, incluidas configuración segura y seguridad del hipervisor	https://core.vmware.com/security
Directiva de seguridad de VMware, alertas de seguridad actualizadas, descargas de seguridad y foros de debate sobre temas de seguridad	http://www.vmware.com/go/security
Directiva de respuestas sobre seguridad corporativa	http://www.vmware.com/support/policies/security_response.html VMware se compromete a ayudar en el mantenimiento de un entorno seguro. Los problemas de seguridad se solucionan oportunamente. La directiva de respuestas sobre seguridad de VMware define nuestro compromiso con la solución de posibles vulnerabilidades en nuestros productos.
Directiva de compatibilidad con software externo	http://www.vmware.com/support/policies/ VMware admite diversos sistemas de almacenamiento y agentes de software, como agentes de copia de seguridad, agentes de administración de sistemas, etc. Para consultar las listas de agentes, herramientas y demás opciones de software compatibles con ESXi, busque en http://www.vmware.com/vmtn/resources/ las guías de compatibilidad de ESXi. La industria ofrece más productos y opciones de configuración de los que VMware puede probar. Si VMware no incluye un producto o una configuración en una guía de compatibilidad, el soporte técnico intenta ayudarle a resolver los problemas, pero no puede garantizar que se pueda usar el producto o la configuración. Siempre evalúe minuciosamente los riesgos para la seguridad que generan los productos o las opciones de configuración no compatibles.
Normas de seguridad y cumplimiento, así como soluciones de partners y contenido detallado sobre virtualización y cumplimiento	https://core.vmware.com/compliance
Información sobre validaciones y certificados de seguridad como CCEVS y FIPS para diferentes versiones de los componentes de vSphere	https://www.vmware.com/support/support-resources/certifications.html
Guías de configuración de seguridad (anteriormente denominadas guías de fortalecimiento) para diferentes versiones de vSphere y otros productos de VMware	https://www.vmware.com/support/support-resources/hardening-guides.html
Informe técnico *Seguridad de VMware vSphere Hypervisor*	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

2 Tareas de administración de permisos y usuarios de vSphere

La autenticación y la autorización rigen el acceso. vCenter Single Sign-On admite la autenticación, lo cual implica que determina si un usuario puede iniciar sesión o no en los componentes de vSphere. Cada usuario también debe estar autorizado para ver o manipular los objetos de vSphere.

vSphere admite varios mecanismos de autorización diferentes, que se analizan en Descripción de la autorización en vSphere. Esta sección se centra en cómo funciona el modelo de permisos de vCenter Server y en cómo realizar tareas de administración de usuarios.

vCenter Server permite un control detallado de la autorización con permisos y funciones. Cuando se asigna un permiso a un objeto en la jerarquía de objetos de vCenter Server, se especifica qué usuario o grupo tiene cuál privilegio sobre ese objeto. Para especificar los privilegios se usan funciones, que son conjuntos de privilegios.

En un principio, solo el usuario administrador del dominio de vCenter Single Sign-On está autorizado a iniciar sesión en el sistema vCenter Server. El dominio predeterminado es vsphere.local y el administrador predeterminado es administrator@vsphere.local. Puede cambiar el dominio predeterminado durante la instalación de vSphere.

El usuario administrador puede proceder de la siguiente manera:

1 Agregue un origen de identidad en el cual los usuarios y grupos estén definidos en vCenter Single Sign-On. Consulte la documentación de *Administrar Platform Services Controller*.

2 Otorgue privilegios a un usuario o un grupo al seleccionar un objeto, como una máquina virtual o un sistema de vCenter Server y asignar una función sobre ese objeto al usuario o al grupo.

Asignar funciones y permisos con vSphere Client (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_m4kg1ebi/uiConfId/49694343/)

Este capítulo incluye los siguientes temas:

- Descripción de la autorización en vSphere
- Administrar permisos para componentes de vCenter
- Permisos globales
- Usar funciones para asignar privilegios

- Prácticas recomendadas para funciones y permisos
- Privilegios necesarios para la realización de tareas comunes

Descripción de la autorización en vSphere

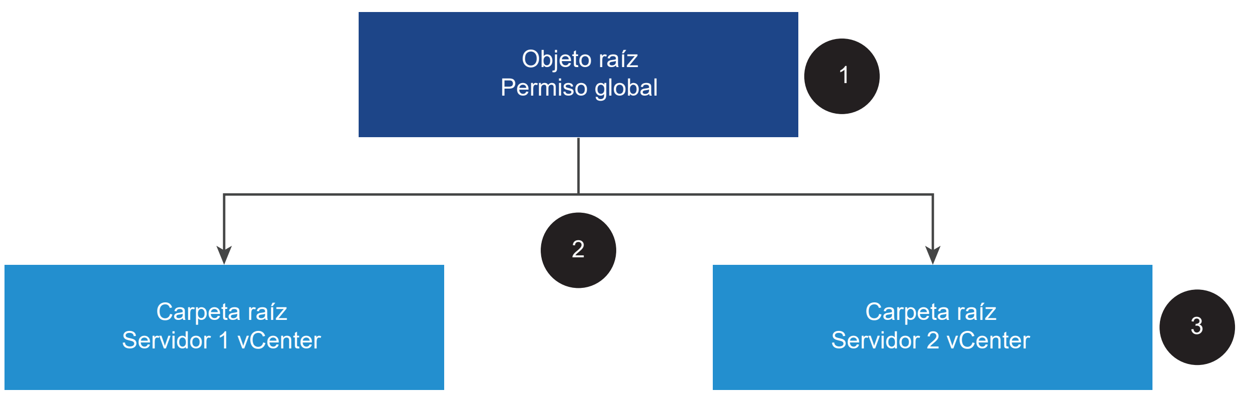
vSphere admite varios modelos para determinar si un usuario puede realizar una tarea. La pertenencia a un grupo en vCenter Single Sign-On determina qué se le permite hacer. Su función respecto de un objeto o su permiso global determinan si se le permite realizar otras tareas.

Descripción general de la autorización

vSphere permite a los usuarios con privilegios otorgar permisos a otros usuarios para realizar tareas. Se pueden utilizar permisos globales o permisos locales de vCenter Server para autorizar a otros usuarios en las instancias individuales de vCenter Server.

En la siguiente figura, se muestra cómo funcionan los permisos globales y locales.

Figura 2-1. Permisos globales y permisos locales



En esta figura:

1 Asigne un permiso global en el nivel de objeto raíz con la opción "Propagar a objetos secundarios" seleccionada.

2 vCenter Server propaga los permisos a las jerarquías de objetos vCenter Server 1 y vCenter Server 2 en el entorno.

3 Un permiso local en la carpeta raíz de vCenter Server 2 anula el permiso global.

Permisos de vCenter Server

El modelo de permisos de los sistemas vCenter Server se basa en la asignación de permisos a los objetos de la jerarquía de objetos. Los usuarios obtienen permisos de las siguientes maneras.

- Desde un permiso específico para el usuario o desde los grupos de los que el usuario es miembro
- Desde un permiso en el objeto o a través de la herencia de permisos de un objeto principal

Cada permiso otorga un conjunto de privilegios a un usuario o grupo; es decir, asigna una función para un objeto seleccionado. Puede usar vSphere Client para agregar permisos. Por ejemplo, puede hacer clic con el botón secundario en una máquina virtual, seleccionar **Agregar permiso** y completar el cuadro de diálogo para asignar una función a un grupo de usuarios. Esa función proporciona a esos usuarios los privilegios correspondientes sobre la máquina virtual.

Permisos globales

Los permisos globales conceden a un usuario o grupo privilegios para ver o administrar todos los objetos en cada una de las jerarquías de inventario de las soluciones de la implementación. Es decir, los permisos globales se aplican a un objeto raíz global que abarca las jerarquías del inventario de soluciones. (Las soluciones incluyen vCenter Server, vRealize Orchestrator, etc.). Los permisos globales también se aplican a objetos globales, como etiquetas y bibliotecas de contenido. Por ejemplo, considere una implementación que consta de dos soluciones: vCenter Server y vRealize Orchestrator. Puede utilizar permisos globales para asignar una función a un grupo de usuarios que tenga privilegios de solo lectura para todos los objetos de las jerarquías de objetos de vCenter Server y vRealize Orchestrator.

Los permisos globales se replican en el dominio de vCenter Single Sign-On (vsphere.local de forma predeterminada). Los permisos globales no proporcionan autorización para servicios administrados a través de grupos de dominios de vCenter Single Sign-On. Consulte Permisos globales.

Pertenencia a grupos de vCenter Single Sign-On

Los miembros de un grupo vsphere.local pueden realizar determinadas tareas. Por ejemplo, se puede llevar a cabo la administración de licencias si se es miembro del grupo LicenseService.Administrators. Consulte la documentación de *Administrar Platform Services Controller*.

Permisos de hosts locales de ESXi

Si administra un host ESXi independiente que no está administrado por un sistema vCenter Server, puede asignar uno de las funciones predefinidas a los usuarios. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*.

Para hosts administrados, asigne funciones al objeto de host ESXi en el inventario de vCenter Server.

Descripción del modelo de permisos de nivel de objetos

Autoriza a un usuario o grupo a realizar tareas en objetos de vCenter Server mediante permisos en el objeto. Desde un punto de vista programático, cuando un usuario intenta realizar una operación, se ejecuta un método de API. vCenter Server comprueba los permisos de ese método para ver si el usuario está autorizado a realizar la operación. Por ejemplo, cuando un usuario

intenta agregar un host, se invoca al método `AddStandaloneHost_Task(addStandaloneHost)`. Este método requiere que la función del usuario tenga el privilegio **Host.Inventario.Agregar host independiente**. Si la comprobación no encuentra este privilegio, se le niega al usuario el permiso para agregar el host.

Los siguientes conceptos son importantes.

Permisos

Cada objeto en la jerarquía de objetos de vCenter Server tiene permisos asociados. Cada permiso especifica en un solo grupo o usuario qué privilegios tiene ese grupo o usuario sobre el objeto.

Usuarios y grupos

En los sistemas vCenter Server se pueden asignar privilegios solo a usuarios autenticados o a grupos de usuarios autenticados. Los usuarios se autentican mediante vCenter Single Sign-On. Los usuarios y los grupos deben definirse en el origen de identidad que vCenter Single Sign-On utiliza para autenticar. Defina usuarios y grupos utilizando las herramientas en su origen de identidad, por ejemplo, Active Directory.

Privilegios

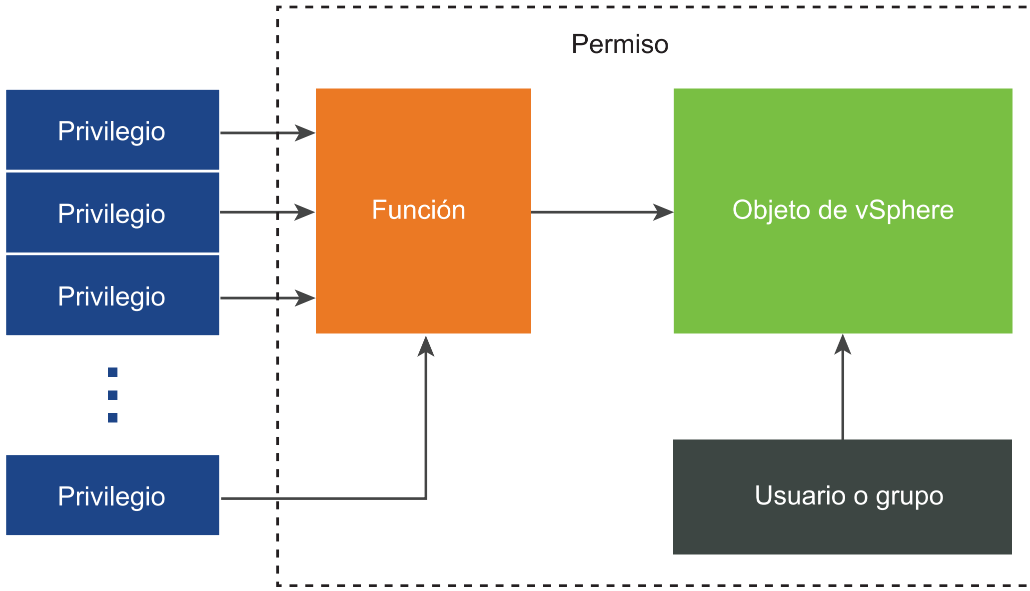
Los privilegios son controles de acceso detallados. Esos privilegios se pueden agrupar en funciones que se pueden asignar a usuarios o grupos posteriormente.

Funciones

Las funciones son conjuntos de privilegios. Las funciones permiten asignar permisos en un objeto en función de un conjunto típico de tareas que realizan los usuarios. En vCenter Server, las funciones predeterminados —tales como Administrador— están predefinidos y no se pueden cambiar. Otras funciones, como Administrador de grupo de recursos, son funciones de muestra predefinidos. Se pueden crear funciones personalizadas, ya sea desde cero o mediante la clonación y la modificación de las funciones de muestra. Consulte Crear una función personalizada.

En la siguiente figura, se muestra cómo se crea un permiso a partir de privilegios y funciones, y se lo asigna a un usuario o grupo para un objeto de vSphere.

Figura 2-2. Permisos de vSphere



Para asignar permisos sobre un objeto, siga estos pasos:

1 Seleccione el objeto en el que desea aplicar el permiso en la jerarquía de objetos de vCenter Server.

2 Seleccione el grupo o el usuario que tendrá los privilegios sobre el objeto.

3 Seleccione privilegios individuales o una función, es decir, un conjunto de privilegios que el grupo o el usuario tendrán sobre el objeto.

   De forma predeterminada, la opción Propagar a objetos secundarios no está seleccionada. Debe activar la casilla para que el grupo o el usuario tengan la función seleccionada para el objeto deseado y sus objetos secundarios.

vCenter Server ofrece funciones predefinidas, que combinan conjuntos de privilegios usados con frecuencia. También puede crear funciones personalizadas mediante la combinación de un conjunto de funciones.

En muchos casos, los permisos deben definirse tanto en un objeto de origen como en un objeto de destino. Por ejemplo, al mover una máquina virtual, se necesitan privilegios en esa máquina virtual, pero también privilegios en el centro de datos de destino.

Consulte la siguiente información.

Para averiguar sobre...	Consulte...
Crear funciones personalizadas.	Crear una función personalizada
Todos los privilegios y los objetos a los que puede aplicar los privilegios	Capítulo 13 Privilegios definidos
Conjuntos de privilegios que se requieren en diferentes objetos para diferentes tareas.	Privilegios necesarios para la realización de tareas comunes

El modelo de permisos de los hosts ESXi independientes es más simple. Consulte Asignar privilegios para hosts ESXi.

Validar usuarios de vCenter Server

Los sistemas vCenter Server que usan un servicio de directorio suelen validar usuarios y grupos en función del dominio del directorio de usuarios. La validación se produce en intervalos regulares especificados en la configuración de vCenter Server. Por ejemplo, supongamos que al usuario Smith se le asigna una función sobre varios objetos. El administrador de dominios cambia el nombre por Smith2. El host concluye que Smith ya no existe y elimina los permisos asociados con ese usuario de los objetos de vSphere en la siguiente validación.

De modo similar, si se elimina el usuario Smith del dominio, todos los permisos asociados con ese usuario se eliminan en la siguiente validación. Si se agrega un nuevo usuario Smith al dominio antes de la siguiente validación, el nuevo usuario Smith reemplaza al antiguo usuario Smith en los permisos sobre cualquier objeto.

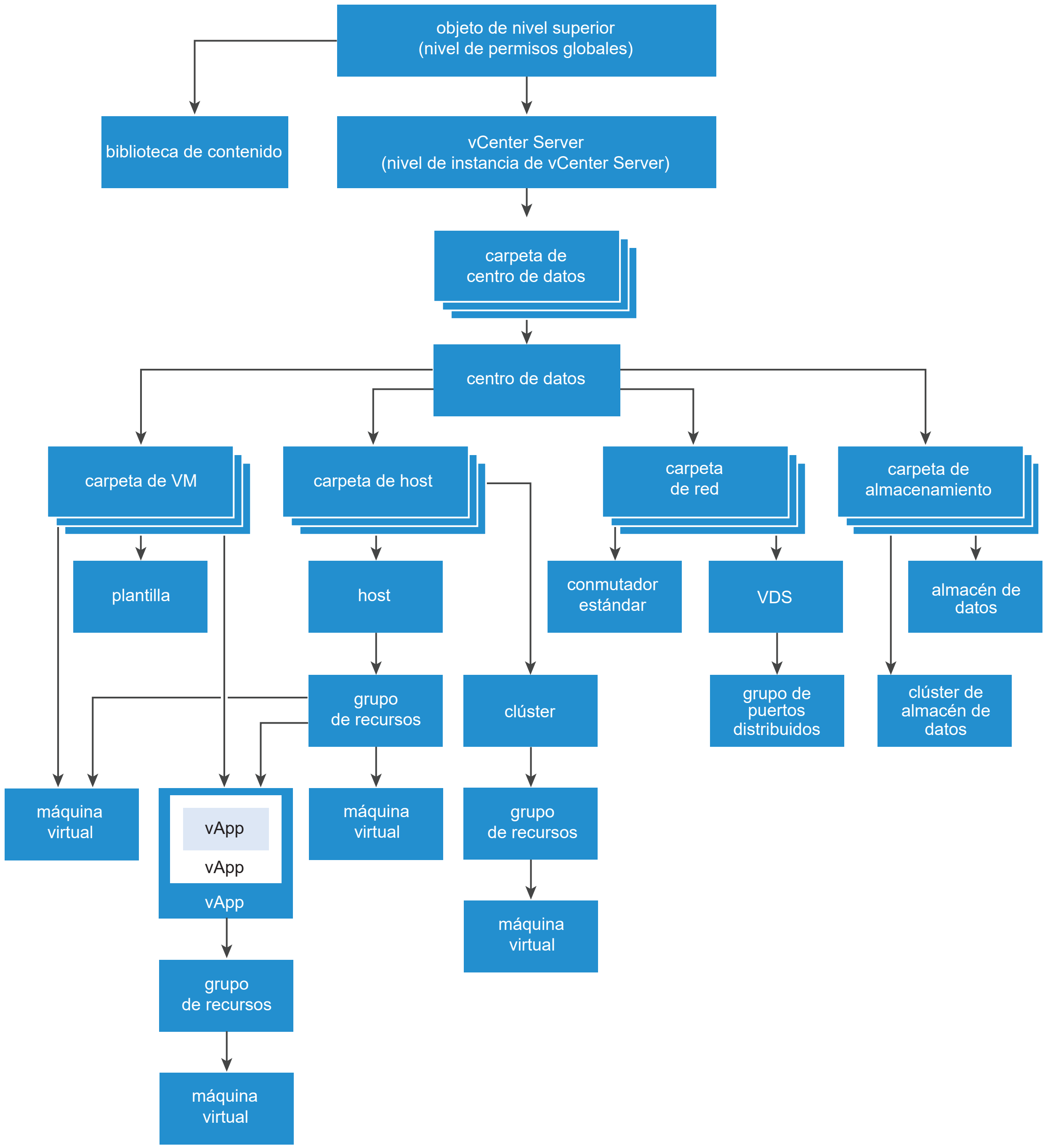
Herencia jerárquica de permisos

Al asignar un permiso a un objeto, se puede elegir si el permiso se propagará en la jerarquía de objetos. La propagación se establece para cada permiso. Es decir, no se aplica universalmente. Los permisos definidos para un objeto secundario siempre anulan los permisos propagados desde los objetos primarios.

La siguiente figura ilustra la jerarquía de inventario y las rutas mediante las cuales pueden propagarse los permisos.

Nota Los permisos globales son compatibles con la asignación de privilegios en soluciones de un objeto raíz global. Consulte Permisos globales.

Figura 2-3. Jerarquía de inventario de vSphere



Acerca de esta figura:

- No se pueden establecer permisos directos en las carpetas de máquina virtual, host, red y almacenamiento. Es decir, estas carpetas actúan como contenedores y, por lo tanto, no son visibles para los usuarios.
- No se pueden establecer permisos en conmutadores estándar.

La mayoría de los objetos del inventario heredan permisos de un único objeto primario de la jerarquía. Por ejemplo, el almacén de datos hereda permisos de la carpeta primaria del almacén o del centro de datos primario. Las máquinas virtuales heredan permisos de la carpeta primaria de máquinas virtuales y del host, clúster o grupo de recursos primario simultáneamente.

Por ejemplo, se pueden establecer permisos para un conmutador distribuido y sus grupos de puertos distribuidos asociados si se configuran permisos para un objeto primario, como una carpeta o un centro de datos. También se debe seleccionar la opción para propagar estos permisos a los objetos secundarios.

Los permisos tienen distintas formas en la jerarquía:

Entidades administradas

Las entidades administradas hacen referencia a los siguientes objetos de vSphere. Las entidades administradas ofrecen operaciones específicas que varían según el tipo de entidad. Los usuarios con privilegios pueden definir permisos en entidades administradas. Consulte la documentación vSphere API para obtener más información sobre los objetos, las propiedades y los métodos de vSphere.

- Clústeres
- Centros de datos
- Almacenes de datos
- Clústeres de almacenes de datos
- Carpetas
- Hosts
- Redes (excepto vSphere Distributed Switch)
- Grupos de puertos distribuidos
- Grupos de recursos
- Plantillas
- Máquinas virtuales
- vSphere vApps

Entidades globales

No se pueden modificar los permisos en entidades que derivan sus permisos del sistema vCenter Server raíz.

- Campos personalizados
- Licencias
- Funciones
- Intervalos de estadísticas

- Sesiones

Configuración de varios permisos

Los objetos pueden tener varios permisos, pero solo es posible tener un permiso por cada usuario o grupo. Por ejemplo, un permiso podría especificar que GroupAdmin tiene la función de administrador en un objeto. Otro permiso podría especificar que GroupVMAdmin tiene la función de administrador de máquinas virtuales en el mismo objeto. Sin embargo, el grupo GroupVMAdmin no puede tener otro permiso para el mismo GroupVMAdmin en este objeto.

Un objeto secundario hereda los permisos de su objeto principal si la propiedad de propagación del objeto principal se establece en true. Un permiso que se establece directamente en un objeto secundario reemplaza el permiso en el objeto principal. Consulte Ejemplo 2: permisos secundarios que anulan permisos primarios.

Si se establecen varios permisos grupales en el mismo objeto y un usuario pertenece a dos o más de esos grupos, pueden ocurrir dos situaciones:

- No se han definido permisos para el usuario directamente en el objeto. En ese caso, el usuario obtiene la unión de los permisos que tienen los grupos en ese objeto.
- Se han definido permisos para el usuario directamente en el objeto. En ese caso, los permisos para el usuario tienen prioridad sobre todos los permisos de grupo.

Ejemplo 1: Herencia de permisos de varios grupos

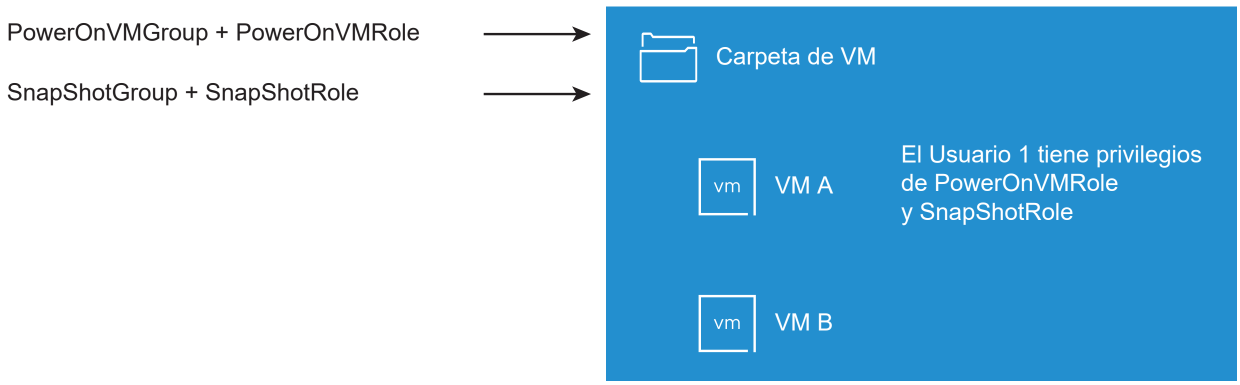
En este ejemplo se muestra cómo un objeto puede heredar varios permisos de los grupos que tienen permisos sobre un objeto primario.

En este ejemplo, se asignan dos permisos sobre el mismo objeto a dos grupos diferentes.

- PowerOnVMRole permite encender las máquinas virtuales.
- SnapShotRole puede crear instantáneas de máquinas virtuales.
- Se asigna PowerOnVMGroup al PowerOnVMRole en la carpeta de máquina virtual; se otorga el permiso para la propagación a objetos secundarios.
- Se asigna SnapShotGroup al SnapShotRole en la carpeta de máquina virtual; se otorga el permiso para la propagación a objetos secundarios.
- No se asignan privilegios específicos al Usuario 1.

El Usuario 1, que pertenece a PowerOnVMGroup y SnapShotGroup, inicia sesión. El Usuario 1 puede encender y crear instantáneas de las máquinas virtuales A y B.

Figura 2-4. Ejemplo 1: Herencia de permisos de varios grupos



Ejemplo 2: permisos secundarios que anulan permisos primarios

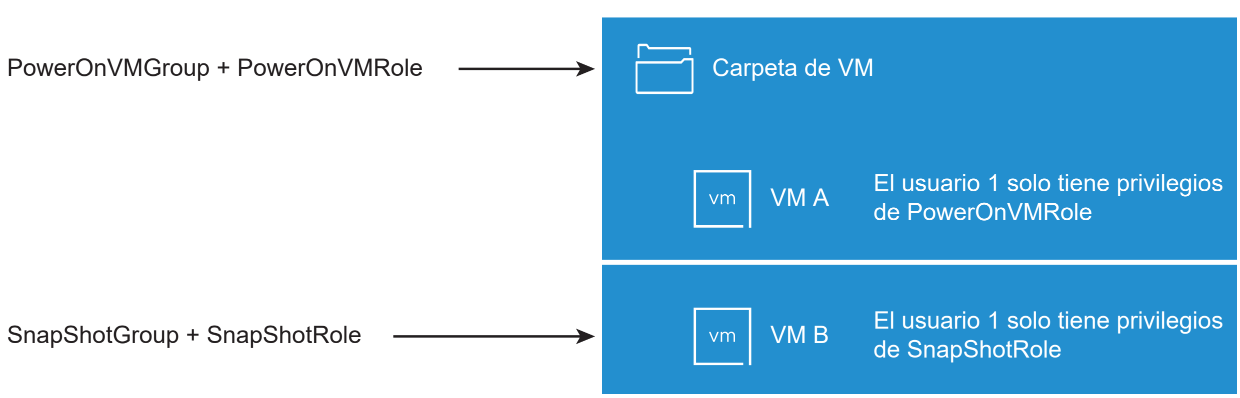
En este ejemplo, se muestra cómo los permisos que se asignan a un objeto secundario pueden anular los permisos que se asignan a un objeto primario. Este comportamiento de anulación se puede utilizar para restringir el acceso de los usuarios a áreas específicas del inventario.

En este ejemplo, los permisos están definidos en dos objetos diferentes de dos grupos distintos.

- PowerOnVMRole permite encender las máquinas virtuales.
- SnapShotRole puede crear instantáneas de máquinas virtuales.
- Se asigna PowerOnVMGroup al PowerOnVMRole en la carpeta de máquina virtual; se otorga el permiso para la propagación a objetos secundarios.
- Se concede SnapShotGroup a SnapShotRole en la máquina virtual B.

El Usuario 1, que pertenece a PowerOnVMGroup y SnapShotGroup, inicia sesión. Ya que SnapShotRole se asigna en un nivel inferior de la jerarquía que PowerOnVMRole, PowerOnVMRole se anula en la máquina virtual B. De esta forma, el Usuario 1 puede encender la máquina virtual A, pero no puede crear instantáneas. El Usuario 1 puede crear instantáneas de la máquina virtual B, pero no puede encenderla.

Figura 2-5. Ejemplo 2: permisos secundarios que anulan permisos primarios



Ejemplo 3: función de usuario que anula la función de grupo

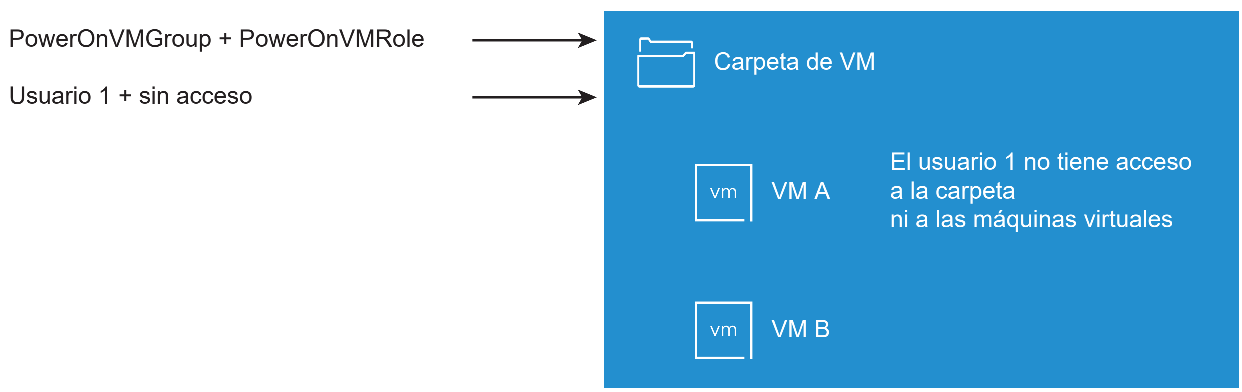
Este ejemplo ilustra cómo la función asignada directamente a un usuario individual anula los privilegios asociados con una función asignada a un grupo.

En este ejemplo, los permisos se definen sobre el mismo objeto. Un permiso asocia un grupo con una función; el otro permiso asocia un usuario individual con una función. El usuario es un miembro del grupo.

- PowerOnVMRole permite encender las máquinas virtuales.
- Se concede PowerOnVMGroup a PowerOnVMRole en la carpeta de máquina virtual.
- Se asigna la función Sin acceso al Usuario 1 en la carpeta de máquina virtual.

El Usuario 1, que pertenece al PowerOnVMGroup, inicia sesión. La función Sin acceso otorgada al Usuario 1 en la carpeta de máquina virtual anula la función asignada al grupo. El Usuario 1 no tiene acceso a la carpeta de máquina virtual o a las máquinas virtuales A y B. Las máquinas virtuales A y B no están visibles en la jerarquía para el Usuario 1.

Figura 2-6. Ejemplo 3: permisos de usuario que anulan permisos de grupo



Administrar permisos para componentes de vCenter

Se establece un permiso sobre un objeto en la jerarquía de objetos de vCenter. Cada permiso asocia el objeto con un grupo o un usuario y con las funciones de acceso de ese grupo o usuario. Por ejemplo, se puede seleccionar un objeto de la máquina virtual, agregar un permiso que asigne la función de solo lectura al Grupo 1 y, a continuación, agregar un segundo permiso que asigne la función de administrador al Usuario 2.

Al asignar una función diferente a un grupo de usuarios en diferentes objetos, se controlan las tareas que esos usuarios pueden realizar en el entorno de vSphere. Por ejemplo, para permitir que un grupo configure memoria del host, seleccione el host y agregue un permiso que otorgue una función a ese grupo, donde se incluya el privilegio **Host. Configuración.Configuración de memoria**.

Para obtener información conceptual sobre los permisos, consulte el análisis en Descripción del modelo de permisos de nivel de objetos.

Puede asignar permisos sobre objetos de diferentes niveles de la jerarquía; por ejemplo, puede asignar permisos a un objeto del host o una carpeta que incluyan todos los objetos del host. Consulte Herencia jerárquica de permisos. Asimismo, puede asignar permisos a un objeto raíz global donde se apliquen los permisos en todos los objetos de todas las soluciones. Consulte Permisos globales.

Agregar un permiso a un objeto de inventario

Después de crear usuarios y grupos, y definir sus funciones, debe asignarlos a los objetos de inventario correspondientes. Para asignar los mismos permisos de propagación a varios objetos al mismo tiempo, mueva los objetos a una carpeta y configure los permisos allí mismo.

Al asignar permisos, los nombres de usuarios y grupos deben coincidir exactamente con los de Active Directory, con distinción de mayúsculas y minúsculas. Si realizó una actualización de versiones anteriores de vSphere y tiene problemas con los grupos, compruebe que no haya inconsistencias de mayúsculas y minúsculas.

Requisitos previos

En el objeto cuyos permisos desea modificar, debe tener una función que incluya el privilegio **Permisos.Modificar permiso**.

Procedimiento

1 Desplácese hasta el objeto para el que desea asignar permisos en el navegador de objetos de vSphere Client.

2 Haga clic en la pestaña **Permisos**.

3 Haga clic en el icono **Agregar permiso**.

4 Seleccione el usuario o el grupo que tendrá los privilegios definidos según la función seleccionada.

   a En el menú desplegable **Usuario**, seleccione el dominio para el usuario o el grupo.

   b Escriba un nombre en el cuadro de búsqueda.

   El sistema buscará nombres de usuarios y nombres de grupos.

   c Seleccione el usuario o grupo.

5 Seleccione una función en el menú desplegable **Función**.

6 (opcional) Para propagar los permisos, seleccione la casilla **Propagar a objetos secundarios**.

   La función se aplicará al objeto seleccionado y se propagará a los objetos secundarios.

7 Haga clic en **Aceptar**.

Cambiar o quitar permisos

Después de que se establece un par usuario/grupo-función para un objeto de inventario, se puede cambiar la función emparejada con el usuario o el grupo, o cambiar la configuración de la casilla **Propagar a objetos secundarios**. También se puede quitar la configuración de permisos.

Procedimiento

1 Desplácese hasta el objeto en el navegador de objetos de vSphere Client.

2 Haga clic en la pestaña **Permisos**.

3 Haga clic en una fila para seleccionar un permiso.

Tarea	Pasos
Cambiar permisos	a Haga clic en el icono **Cambiar función**. b En el menú desplegable **Función**, seleccione una función para el usuario o el grupo. c Active o desactive la casilla **Propagar a objetos secundarios** para cambiar la herencia de permisos. d Haga clic en **Aceptar**.
Quitar permisos	Haga clic en el icono **Quitar permiso**.

Cambiar la configuración de validación de usuarios

vCenter Server valida de forma periódica la lista de usuarios y grupos con los usuarios y grupos del directorio de usuarios. A continuación, quita los usuarios y los grupos que ya no existen en el dominio. Se puede deshabilitar la validación o cambiar el intervalo entre las validaciones. Si tiene dominios con miles de usuarios o grupos, o bien si las búsquedas tardan mucho en completarse, considere ajustar la configuración de la búsqueda.

Para las versiones de vCenter Server anteriores a vCenter Server 5.0, esta configuración se aplica en un Active Directory asociado con vCenter Server. Para las versiones vCenter Server 5.0 y posteriores, esta configuración se aplica a los orígenes de identidad de vCenter Single Sign-On.

Nota Este procedimiento se aplica únicamente a las listas de usuarios de vCenter Server. No puede buscar listas de usuarios de ESXi de la misma manera.

Procedimiento

1 Desplácese hasta el sistema vCenter Server en el navegador de objetos de vSphere Client.

2 Seleccione **Configurar** y haga clic en **Configuración > General**.

3 Haga clic en **Editar** y seleccione **Directorio de usuarios**.

4 Cambie los valores según sea necesario y haga clic en **Guardar**.

Opción	Descripción
Tiempo de espera del directorio de usuarios	Intervalo de tiempo de espera en segundos para la conexión al servidor de Active Directory. Este valor especifica la cantidad máxima de tiempo que vCenter Server permite para la ejecución de una búsqueda en el dominio seleccionado. La búsqueda en dominios grandes puede tardar mucho.
Límite de consulta	Active para establecer un número máximo de usuarios y grupos que mostrará vCenter Server.
Tamaño del límite de consulta	Cantidad máxima de usuarios y grupos del dominio seleccionado que vCenter Server muestra en el cuadro de diálogo **Seleccionar usuarios o grupos**. Si escribe 0 (cero), aparecen todos los usuarios y grupos.
Validación	Desactive para deshabilitar la validación.
Período de validación	Especifica la frecuencia con que vCenter Server valida permisos (en minutos).

Permisos globales

Los permisos globales se aplican a un objeto raíz global que expande soluciones. En un SDDC local, los permisos globales pueden abarcar tanto vCenter Server como vRealize Orchestrator. Sin embargo, para vSphere SDDC, los permisos globales se aplican a objetos globales, como etiquetas y bibliotecas de contenido.

Puede asignar permisos globales a usuarios o grupos, y decidir qué función asignar a cada usuario o grupo. La función determina el conjunto de privilegios que el usuario o el grupo tienen para todos los objetos de la jerarquía. Puede asignar una función predefinida o crear funciones personalizadas. Consulte Usar funciones para asignar privilegios.

Es importante distinguir entre los permisos de vCenter Server y los permisos globales.

Permisos de vCenter Server

Generalmente, se aplica un permiso a un objeto de inventario de vCenter Server, como una máquina virtual. Cuando se realiza esta acción, se especifica que el usuario o grupo tenga una función (conjunto de privilegios), sobre el objeto.

Permisos globales

Los permisos globales conceden a un usuario o grupo privilegios para ver o administrar todos los objetos en cada una de las jerarquías de inventario de la implementación. Los permisos globales también se aplican a objetos globales, como etiquetas y bibliotecas de contenido. Consulte Permisos en objetos de etiqueta.

Si asigna un permiso global y no selecciona Propagar, los usuarios o grupos asociados con este permiso no tendrán acceso a los objetos de la jerarquía. Solo podrán acceder a algunas funcionalidades globales, como la creación de funciones.

Importante Utilice los permisos globales con atención. Compruebe si realmente desea asignar permisos para todos los objetos en todas las jerarquías del inventario.

Agregar permisos globales

Se pueden utilizar permisos globales para otorgar a un usuario o un grupo privilegios sobre todos los objetos de todas las jerarquías del inventario de la implementación.

Importante Utilice los permisos globales con atención. Compruebe si realmente desea asignar permisos para todos los objetos en todas las jerarquías del inventario.

Requisitos previos

Para realizar esta tarea, se deben tener los privilegios **Permisos.Modificar permisos** en el objeto raíz de todas las jerarquías del inventario.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione **Administración** y haga clic en **Permisos globales** en el área de control de acceso.

3 Haga clic en el icono **Agregar permiso**.

4 Seleccione el usuario o el grupo que tendrá los privilegios definidos según la función seleccionada.

   a En el menú desplegable **Usuario**, seleccione el dominio para el usuario o el grupo.

   b Escriba un nombre en el cuadro de búsqueda.

   El sistema buscará nombres de usuarios y nombres de grupos.

   c Seleccione el usuario o grupo.

5 Seleccione una función en el menú desplegable **Función**.

6 Decida si desea propagar los permisos mediante la selección de la casilla **Propagar a objetos secundarios**.

   Si asigna un permiso global y no selecciona **Propagar a objetos secundarios**, los usuarios o grupos asociados con este permiso no tendrán acceso a los objetos de la jerarquía. Solo podrán acceder a algunas funcionalidades globales, como la creación de funciones.

7 Haga clic en **Aceptar**.

Permisos en objetos de etiqueta

En la jerarquía de objetos de vCenter Server, los objetos de etiqueta no son objetos secundarios de vCenter Server, sino que se crean al nivel superior de vCenter Server. En los entornos que tienen varias instancias de vCenter Server, los objetos de etiqueta se comparten en las instancias de vCenter Server. El funcionamiento de los permisos para los objetos de etiqueta es distinto al de los permisos para otros objetos de la jerarquía de objetos de vCenter Server.

Solo se aplican los permisos globales o los permisos asignados al objeto de etiqueta

Si otorga permisos a un usuario en un objeto de inventario de vCenter Server, como una máquina virtual, ese usuario puede realizar las tareas asociadas con el permiso. Sin embargo, el usuario no puede realizar operaciones de etiquetado en el objeto.

Por ejemplo, si otorga el privilegio **Asignar etiqueta de vSphere** al usuario Dana en el host TPA, ese permiso no afecta la posibilidad de Dana de asignar etiquetas en el host TPA. Dana debe tener el privilegio **Asignar etiqueta de vSphere** en el nivel superior, es decir, un permiso global, o debe tener el privilegio para el objeto de etiqueta.

Tabla 2-1. Cómo influyen los permisos globales y los permisos de objeto de etiqueta en lo que pueden hacer los usuarios

Permiso global	Permiso de nivel de etiqueta	Permiso de nivel de objeto de vCenter Server	Permiso efectivo
No hay privilegios de etiquetado asignados.	Dana tiene los privilegios **Asignar o desasignar etiqueta de vSphere** para la etiqueta.	Dana tiene los privilegios **Eliminar etiqueta de vSphere** en el host ESXi TPA.	Dana tiene los privilegios **Asignar o desasignar etiqueta de vSphere** para la etiqueta.
Dana tiene los privilegios **Asignar o desasignar etiqueta de vSphere**.	No hay privilegios asignados para la etiqueta.	Dana tiene los privilegios **Eliminar etiqueta de vSphere** en el host ESXi TPA.	Dana tiene los privilegios globales **Asignar o desasignar etiqueta de vSphere**. Eso incluye privilegios en el nivel de etiqueta.
No hay privilegios de etiquetado asignados.	No hay privilegios asignados para la etiqueta.	Dana tiene los privilegios **Asignar o desasignar etiqueta de vSphere** en el host ESXi TPA.	Dana no tiene privilegios de etiquetado en ningún objeto, incluido el host TPA.

Los permisos globales complementan los permisos de objeto de etiqueta

Los permisos globales, es decir, los permisos que están asignados en el objeto de nivel superior, complementan los permisos en los objetos de etiqueta cuando los permisos de los objetos de etiqueta tienen más restricciones. Los permisos de vCenter Server no influyen en los objetos de etiqueta.

Por ejemplo, suponga que asigna el privilegio **Eliminar etiqueta de vSphere** al usuario Robin en el nivel superior mediante el uso de permisos globales. Para la producción de la etiqueta, no asigna el privilegio **Eliminar etiqueta de vSphere** a Robin. En ese caso, Robin tiene el privilegio para la producción de etiqueta porque tiene el permiso global, que se propaga desde el nivel superior. No se pueden restringir los privilegios a menos que se modifique el permiso global.

Tabla 2-2. Los permisos globales complementan los permisos de nivel de etiqueta

Permiso global	Permiso de nivel de etiqueta	Permiso efectivo
Robin tiene los privilegios **Eliminar etiqueta de vSphere**.	Robin no tiene los privilegios **Eliminar etiqueta de vSphere** para la etiqueta.	Robin tiene los privilegios **Eliminar etiqueta de vSphere**.
No hay privilegios de etiquetado asignados.	Robin no tiene los privilegios **Eliminar etiqueta de vSphere** asignados para la etiqueta.	Robin no tiene los privilegios **Eliminar etiqueta de vSphere**.

Los permisos de nivel de etiqueta pueden extender los permisos globales

Se pueden utilizar permisos de nivel de etiqueta para extender los permisos globales. Eso significa que los usuarios pueden tener un permiso global y un permiso de nivel de etiqueta en una etiqueta.

Nota Este comportamiento es diferente de la forma vCenter Server se heredan los privilegios. En vCenter Server, los permisos definidos para un objeto secundario siempre anulan los permisos propagados desde los objetos primarios.

Tabla 2-3. Los permisos globales extienden los permisos de nivel de etiqueta

Permiso global	Permiso de nivel de etiqueta	Permiso efectivo
Lee tiene el privilegio **Asignar o desasignar etiqueta de vSphere**.	Lee tiene el privilegio **Eliminar etiqueta de vSphere**.	Lee tiene los privilegios **Asignar etiqueta de vSphere** y **Eliminar etiqueta de vSphere** para la etiqueta.
No hay privilegios de etiquetado asignados.	Lee tiene el privilegio **Eliminar etiqueta de vSphere** asignado para la etiqueta.	Lee tiene el privilegio **Eliminar etiqueta de vSphere** para la etiqueta.

Usar funciones para asignar privilegios

Una función es un conjunto predefinido de privilegios. Los privilegios definen derechos para realizar acciones y propiedades de lectura. Por ejemplo, la función de Administrador de máquinas virtuales permite que los usuarios lean y cambien los atributos de la máquina virtual.

Al asignar permisos, se establece un par entre un usuario o grupo y una función, y se asocia ese par a un objeto del inventario. Un mismo usuario o grupo puede tener diferentes funciones para distintos objetos del inventario.

Por ejemplo, supongamos que tiene dos grupos de recursos en el inventario, el Grupo A y el Grupo B. Puede asignar al grupo Ventas la función de usuario de la máquina virtual para el Grupo A y la función de solo lectura para el Grupo B. Con estas asignaciones, los usuarios del grupo Ventas pueden encender las máquinas virtuales del Grupo A, pero solo pueden ver las del Grupo B.

vCenter Server proporciona funciones del sistema y funciones de muestra de forma predeterminada.

Funciones del sistema

Las funciones del sistema son permanentes. No se pueden editar los privilegios asociados con estas funciones.

Funciones de muestra

VMware proporciona funciones de muestra para ciertas combinaciones de tareas frecuentes. Estas funciones se pueden clonar, modificar o quitar.

Nota Para evitar perder la configuración predefinida en una función de muestra, primero clone la función y, a continuación, realice las modificaciones en el clon. No se puede restablecer la muestra a su configuración predeterminada.

Los usuarios pueden programar tareas únicamente si tienen una función que incluya privilegios para realizar esa tarea en el momento de crearla.

Nota Los cambios en las funciones y en los privilegios se aplican de inmediato, incluso si los usuarios involucrados iniciaron sesión. La excepción son las búsquedas, para las cuales los cambios se aplican una vez que el usuario cierra la sesión y vuelve a iniciarla.

Funciones personalizadas en vCenter Server y ESXi

Se pueden crear funciones personalizadas para vCenter Server y todos los objetos que administra, o bien para hosts individuales.

Funciones personalizadas de vCenter Server (recomendado)

Si se desean crear funciones personalizadas, se pueden utilizar las opciones de edición de funciones en vSphere Client para crear conjuntos de privilegios que se adapten a los requisitos.

Funciones personalizadas de ESXi

Se pueden crear funciones personalizadas para hosts individuales mediante la utilización de una CLI o de VMware Host Client. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*. No se puede acceder a las funciones de host personalizadas desde vCenter Server.

Si administra los hosts ESXi mediante vCenter Server, no mantenga las funciones personalizadas en el host y en vCenter Server. Defina las funciones en el nivel de vCenter Server.

Cuando se administra un host por medio de vCenter Server, los permisos asociados con ese host se crean desde vCenter Server y se almacenan en vCenter Server. Si se conecta directamente a un host, solo están disponibles las funciones que se crearon de forma directa en el host.

Nota Cuando se agrega una función personalizada y no se le asignan privilegios, la función creada es de solo lectura con tres privilegios definidos por el sistema: **Sistema.Anónimo**, **Sistema.Ver** y **Sistema.Leer**. Estos privilegios no están visibles en vSphere Client, pero se utilizan para leer ciertas propiedades de algunos objetos administrados. Todas las funciones predefinidas en vCenter Server contienen estos tres privilegios definidos por el sistema. Consulte la documentación sobre *vSphere Web Services API* para obtener más información.

Crear una función personalizada

Puede crear funciones personalizadas de vCenter Server que se adapten a las necesidades de control de acceso del entorno. Puede crear una función o clonar una función existente.

Puede crear o editar una función en un sistema vCenter Server que forme parte del mismo dominio de vCenter Single Sign-On que los otros sistemas vCenter Server. VMware Directory Service (vmdir) propaga los cambios que se realicen en la función a todos los demás sistemas vCenter Server en el grupo. Las asignaciones de funciones a usuarios y objetos específicos no se comparten en los sistemas vCenter Server.

Requisitos previos

Compruebe haber iniciado sesión como un usuario con privilegios de administrador.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione **Administración** y haga clic en **Funciones** en el área **Control de acceso**.

3 Cree la función:

Opción	Descripción
Para crear una función	Haga clic en el icono **Crear acción de función**.
Para crear la función mediante clonación	Seleccione una función y haga clic en el icono **Clonar acción de función**.

   Consulte Funciones del sistema vCenter Server para obtener más información.

4 Seleccione privilegios para la función o anule la selección de estos.

   Consulte Capítulo 13 Privilegios definidos para obtener más información.

   Nota Cuando se crea una función clonada, no se pueden cambiar los privilegios. Para cambiar los privilegios, seleccione la función clonada después de crearla y haga clic en el icono **Editar acción de función**.

5 Escriba un nombre para la nueva función.

6 Haga clic en **Finalizar**.

Pasos siguientes

Ahora puede crear permisos mediante la selección de un objeto y la asignación de la función a un usuario o un grupo para dicho objeto.

Funciones del sistema vCenter Server

Una función es un conjunto predefinido de privilegios. Al añadir permisos a un objeto, se empareja un usuario o un grupo con una función. vCenter Server incluye varias funciones del sistema que no se pueden cambiar.

vCenter Server ofrece algunas funciones predeterminadas. Los privilegios asociados con las funciones predeterminadas no se pueden cambiar. Las funciones predeterminadas se organizan en una jerarquía. Cada función hereda los privilegios de la función anterior. Por ejemplo, el rol de administrador hereda los privilegios del rol de solo lectura.

La jerarquía de la función vCenter Server también incluye varias funciones de muestra. Puede clonar una función de muestra para crear una función similar.

Si crea una función, esta no hereda los privilegios de ninguna de las funciones del sistema.

Función de administrador

Los usuarios con la función de administrador para un objeto tienen permiso de ver el objeto y realizar todas las acciones posibles en él. Esta función también incluye todos los privilegios inherentes a la función de solo lectura. Si tiene la función de administrador en un objeto, puede asignar privilegios a grupos y usuarios individuales.

Si actúa con función de administrador en vCenter Server, puede asignar privilegios a los usuarios y grupos del origen de identidad predeterminado de vCenter Single Sign-On. Consulte la documentación de *Administrar Platform Services Controller* para obtener información sobre los servicios de identidad admitidos.

De forma predeterminada, el usuario administrator@vsphere.local tiene la función de administrador tanto en vCenter Single Sign-On como en vCenter Server después de la instalación. Ese usuario puede asociar otros usuarios con la función de administrador en vCenter Server.

Función de solo lectura

Los usuarios con la función Solo lectura para un objeto tienen permiso de ver el estado y los detalles del objeto. Por ejemplo, los usuarios con esta función pueden ver atributos de máquinas virtuales, hosts y grupos de recursos, pero no pueden ver la consola remota para un host. Las acciones desde los menús y las barras de herramientas no están permitidas.

Función Sin acceso

Los usuarios con la función Sin acceso a un objeto no pueden ver ni cambiar ese objeto de ninguna manera. Los usuarios y grupos nuevos tienen asignada esta función de forma predeterminada. Es posible cambiar la función de un solo objeto a la vez.

El administrador del dominio de vCenter Single Sign-On, administrator@vsphere.local de manera predeterminada, el usuario raíz y vpxuser tienen asignada la función Administrador de manera predeterminada. De manera predeterminada, se asigna la función Sin acceso a los otros usuarios.

La práctica recomendada es crear un usuario en el nivel raíz y asignar la función Administrador a ese usuario. Después de crear un usuario designado con privilegios de Administrador, puede quitar el usuario raíz de cualquiera de los permisos o cambiar la función a Sin acceso.

Prácticas recomendadas para funciones y permisos

Siga las prácticas recomendadas para funciones y permisos a fin de maximizar la seguridad y la facilidad de administración del entorno de vCenter Server.

Siga estas prácticas recomendadas para configurar funciones y permisos en un entorno de vCenter Server:

- Siempre que sea posible, asigne una función a un grupo en lugar de hacerlo a usuarios individuales.
- Otorgue permisos solo en los objetos en los que esto sea necesario y asigne privilegios solo a los usuarios o grupos que deban tenerlos. Use una cantidad mínima de permisos para facilitar la comprensión y la administración de la estructura de permisos.
- Si asigna una función restrictiva a un grupo, compruebe que el grupo no contenga el usuario administrador u otros usuarios con privilegios administrativos. De lo contrario, podría restringir los privilegios de administradores de forma accidental en partes de la jerarquía de inventario en las que asignó la función restrictiva al grupo.
- Use carpetas para agrupar objetos. Por ejemplo, para conceder un permiso de modificación para un grupo de hosts y ver dicho permiso en otro conjunto de hosts, coloque cada conjunto de hosts en una carpeta.
- Tenga cuidado al agregar un permiso a los objetos raíz de vCenter Server. Los usuarios con privilegios en nivel de raíz tienen acceso a los datos globales en vCenter Server, como funciones, atributos personalizados y configuración de vCenter Server.
- Considere la posibilidad de habilitar la propagación al asignar los permisos a un objeto. La propagación garantiza que los objetos nuevos de la jerarquía de objetos hereden los permisos. Por ejemplo, puede asignar un permiso a una carpeta de máquina virtual y habilitar la propagación para garantizar que el permiso se aplique a todas las máquinas virtuales de la carpeta.
- Utilice la función Sin acceso para enmascarar determinadas áreas de la jerarquía. La función Sin acceso restringe el acceso a los usuarios o grupos que tengan esa función.
- Los cambios que se realicen en las licencias se propagan del siguiente modo:
  - A todos los sistemas vCenter Server que estén vinculados al mismo Platform Services Controller.

  - A las instancias de Platform Services Controller en el mismo dominio de vCenter Single Sign-On.
- La propagación de las licencias se produce incluso si el usuario no tiene privilegios en todos los sistemas vCenter Server.

Privilegios necesarios para la realización de tareas comunes

Muchas tareas necesitan permisos en varios objetos del inventario. Si el usuario que intenta realizar la tarea únicamente tiene privilegios en un solo objeto, la tarea no se puede completar de forma correcta.

En la siguiente tabla, se enumeran las tareas comunes que necesitan más de un privilegio. Puede agregar permisos a los objetos del inventario mediante el emparejamiento de un usuario con una de las funciones predefinidas o con varios privilegios. Si prevé que asignará un conjunto de privilegios varias veces, cree funciones personalizadas.

Consulte la documentación de referencia de la API de *vSphere Web Services* para obtener información sobre cómo se asignan las operaciones de la interfaz de usuario de vSphere Client a las llamadas API y los privilegios necesarios para realizar operaciones. Por ejemplo, la documentación de la API del método `AddHost_Task(addHost)` especifica que se requiere el privilegio **Host.Inventory.AddHostToCluster** para agregar un host a un clúster.

Si la tarea que desea realizar no figura en la tabla, las siguientes reglas explican dónde debe asignar permisos para permitir determinadas operaciones:

- Cualquier operación que consume espacio de almacenamiento requiere el privilegio **Almacén de datos.Asignar espacio** en el almacén de datos de destino, así como el privilegio para realizar la operación en sí. Debe tener estos privilegios, por ejemplo, cuando se crea un disco virtual o toma una instantánea.
- Mover un objeto en la jerarquía del inventario requiere los privilegios apropiados en el objeto mismo, el objeto primario de origen (como una carpeta o un clúster) y el objeto primario de destino.
- Cada host o clúster tiene su propio grupo de recursos implícito, que contiene todos los recursos de ese host o clúster. Para implementar una máquina virtual directamente en un host o un clúster, se necesita el privilegio **Recurso.Asignar máquina virtual a un grupo de recursos**.

Tabla 2-4. Privilegios necesarios para la realización de tareas comunes

Tarea	Privilegios necesarios	Función aplicable
Crear una máquina virtual	En la carpeta de destino o el centro de datos: ■ **Máquina virtual .Inventario.Crear nuevo** ■ **Máquina virtual.Configuración.Agregar disco nuevo** (si se está creando un nuevo disco virtual) ■ **Máquina virtual.Configuración.Agregar un disco existente** (si se está usando un disco virtual existente) ■ **Máquina virtual.Configuración.Configurar dispositivo sin formato** (si se está usando un dispositivo de acceso directo RDM o SCSI)	Administrador
	En el host, clúster o grupo de recursos de destino: **Recurso.Asignar máquina virtual a grupo de recursos**	Administrador del grupo de recursos o Administrador
	En el almacén de datos de destino o la carpeta que contiene el almacén de datos: **Almacén de datos.Asignar espacio**	Administrador o Consumidor del almacén de datos
	En la red a la cual se asignará la máquina virtual: **Red.Asignar red**	Administrador o Consumidor de la red
Encender una máquina virtual	En el centro de datos en el que se implementa la máquina virtual: **Máquina virtual .Interacción .Encender**	Administrador o Usuario avanzado de la máquina virtual
	En la máquina virtual o en una carpeta de máquinas virtuales: **Máquina virtual .Interacción .Encender**	
Implementación de una máquina virtual desde una plantilla	En la carpeta de destino o el centro de datos: ■ **Máquina virtual .Inventario.Crear a partir de existente** ■ **Máquina virtual.Configuración.Agregar disco nuevo**	Administrador
	En una plantilla o una carpeta de plantillas: **Máquina virtual .Aprovisionamiento.Implementar plantilla**	Administrador
	En el host, clúster o grupo de recursos de destino: **Recurso.Asignar máquina virtual a grupo de recursos**	Administrador
	En el almacén de datos de destino o en la carpeta de almacenes de datos: **Almacén de datos.Asignar espacio**	Administrador o Consumidor del almacén de datos
	En la red a la cual se asignará la máquina virtual: **Red.Asignar red**	Administrador o Consumidor de la red
Creación de una snapshot de una máquina virtual	En la máquina virtual o en una carpeta de máquinas virtuales: **Máquina virtual .Administración de instantáneas. Crear instantánea**	Administrador o Usuario avanzado de la máquina virtual

Tabla 2-4. Privilegios necesarios para la realización de tareas comunes (continuación)

Tarea	Privilegios necesarios	Función aplicable
Transferencia de una máquina virtual a un grupo de recursos	En la máquina virtual o en una carpeta de máquinas virtuales: ■ **Recurso.Asignar máquina virtual a grupo de recursos** ■ **Máquina virtual .Inventario.Mover**	Administrador
	En el grupo de recursos de destino: **Recurso.Asignar máquina virtual a grupo de recursos**	Administrador
Instalar un sistema operativo invitado en una máquina virtual	En la máquina virtual o en una carpeta de máquinas virtuales: ■ **Máquina virtual .Interacción .Responder pregunta** ■ **Máquina virtual .Interacción .Interacción de consola** ■ **Máquina virtual .Interacción .Conexión de dispositivos** ■ **Máquina virtual .Interacción .Apagar** ■ **Máquina virtual .Interacción .Encender** ■ **Máquina virtual .Interacción .Restablecer** ■ **Máquina virtual .Interacción .Configurar medio de CD** (si se está instalando desde un CD) ■ **Máquina virtual .Interacción .Configurar medio de disquete** (si se está instalando desde un disquete) ■ **Máquina virtual .Interacción .Instalar VMware Tools**	Administrador o Usuario avanzado de la máquina virtual
	En un almacén de datos que contiene la imagen ISO de los medios de instalación: **Almacén de datos.Examinar almacén de datos** (si se está instalando desde una imagen ISO en un almacén de datos) En el almacén de datos en el que se cargue la imagen ISO de los medios de instalación: ■ **Almacén de datos.Examinar almacén de datos** ■ **Almacén de datos.Operaciones de archivos de bajo nivel**	Administrador o Usuario avanzado de la máquina virtual
Migración de una máquina virtual con vMotion	En la máquina virtual o en una carpeta de máquinas virtuales: ■ **Recurso.Migrar máquina virtual encendida** ■ **Recurso.Asignar máquina virtual a un grupo de recursos** (si el destino es un grupo de recursos distinto al de origen)	Administrador del grupo de recursos o Administrador
	En el host, clúster o grupo de recursos de destino (si es distinto al de origen): **Recurso.Asignar máquina virtual a grupo de recursos**	Administrador del grupo de recursos o Administrador
Migración en frío (reubicación) de una máquina virtual	En la máquina virtual o en una carpeta de máquinas virtuales: ■ **Recurso.Migrar máquina virtual apagada** ■ **Recurso.Asignar máquina virtual a grupo de recursos** (si el destino es un grupo de recursos distinto al de origen)	Administrador del grupo de recursos o Administrador
	En el host, clúster o grupo de recursos de destino (si es distinto al de origen): **Recurso.Asignar máquina virtual a grupo de recursos**	Administrador del grupo de recursos o Administrador

Tabla 2-4. Privilegios necesarios para la realización de tareas comunes (continuación)

Tarea	Privilegios necesarios	Función aplicable
	En el almacén de datos de destino (si es distinto al de origen): **Almacén de datos.Asignar espacio**	Administrador o Consumidor del almacén de datos
Migración de una máquina virtual con Storage vMotion	En la máquina virtual o en una carpeta de máquinas virtuales: **Recurso.Migrar máquina virtual encendida**	Administrador del grupo de recursos o Administrador
	En el almacén de datos de destino: **Almacén de datos.Asignar espacio**	Administrador o Consumidor del almacén de datos
Transferencia de un host a un clúster	En el host: **Host.Inventario.Agregar host a clúster**	Administrador
	En el clúster de destino: ■ **Host.Inventario.Agregar host a clúster** ■ **Host.Inventario.Modificar clúster**	Administrador
Agregar un solo host a un centro de datos mediante vSphere Client o agregar un solo host a un clúster mediante PowerCLI o la API (aprovechando la API de addHost)	En el host: **Host.Inventario.Agregar host a clúster**	Administrador
	En el clúster: ■ **Host.Inventario.Modificar clúster** ■ **Host.Inventario.Agregar host a clúster**	Administrador
	En el centro de datos: **Host.Inventario.Agregar host independiente**	Administrador
Agregar varios hosts a un clúster (disponible a partir de vSphere 6,7 Update 1)	En el clúster: ■ **Host.Inventario.Modificar clúster** ■ **Host.Inventario.Agregar host a clúster**	Administrador
	En el centro de datos principal del clúster (con propagación): ■ **Host.Inventario.Agregar host independiente** ■ **Host.Inventario.Mover host** ■ **Host.Inventario.Modificar clúster** ■ **Host.Configuración.Mantenimiento**	Administrador
Cifrado de una máquina virtual	Las tareas de cifrado son solo posibles en los entornos que incluyen vCenter Server. Además, el host ESXi debe tener un modo de cifrado habilitado para la mayoría de las tareas de cifrado. El usuario que realiza la tarea debe contar con los privilegios correspondientes. Un conjunto de privilegios **Operaciones criptográficas** permite un control detallado. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado.	Administrador

Proteger hosts ESXi

3

La arquitectura del hipervisor de ESXi tiene muchas características de seguridad incorporadas, como aislamiento de la CPU, aislamiento de la memoria y aislamiento del dispositivo. Es posible configurar características adicionales, como el modo de bloqueo, el reemplazo de certificados y la autenticación de tarjeta inteligente para una seguridad mejorada.

Un host ESXi también está protegido con un firewall. Puede abrir los puertos para el tráfico entrante y saliente según sea necesario, pero debe restringir el acceso a los servicios y los puertos. El modo de bloqueo de ESXi y la limitación de acceso a ESXi Shell puede contribuir aún más a un entorno más seguro. Los hosts ESXi participan en la infraestructura de certificados. Los hosts están aprovisionados con certificados firmados por VMware Certificate Authority (VMCA) de forma predeterminada.

Consulte el informe técnico VMware *Seguridad de VMware vSphere Hypervisor* para obtener información adicional sobre la seguridad de ESXi.

Nota ESXi no se basa en el kernel de Linux ni en una distribución convencional de Linux. Utiliza sus propias herramientas de software y kernel especializadas de VMware, que se proporcionan como una unidad independiente, y no contiene aplicaciones ni componentes de las distribuciones de Linux.

Este capítulo incluye los siguientes temas:

- Recomendaciones generales sobre seguridad de ESXi
- Administrar certificados para hosts ESXi
- Personalizar hosts con el perfil de seguridad
- Asignar privilegios para hosts ESXi
- Usar Active Directory para administrar usuarios de ESXi
- Usar vSphere Authentication Proxy
- Configurar la autenticación de tarjeta inteligente de ESXi
- Usar ESXi Shell
- Arranque seguro UEFI para hosts ESXi
- Proteger hosts ESXi con el módulo de plataforma de confianza

- Archivos de registro de ESXi

Recomendaciones generales sobre seguridad de ESXi

Para proteger un host ESXi contra la intromisión no autorizada o el uso incorrecto, VMware impone restricciones sobre varios parámetros, opciones de configuración y actividades. Es posible reducir las restricciones para cumplir con las necesidades de configuración del usuario. Si lo hace, asegúrese de trabajar en un entorno de confianza y tome otras medidas de seguridad.

Características de seguridad integradas

Los riesgos para los hosts se mitigan desde el comienzo de la siguiente manera:

- ESXi Shell y SSH están deshabilitados de forma predeterminada.
- Solo una cantidad limitada de puertos de firewall está abierta de forma predeterminada. Puede abrir de forma explícita puertos de firewall adicionales asociados con dispositivos específicos.
- ESXi ejecuta solo los servicios que son fundamentales para administrar sus funciones. La distribución está limitada a las características necesarias para ejecutar ESXi.
- De forma predeterminada, todos los puertos que no son necesarios para el acceso de administración al host están cerrados. Abra los puertos si necesita servicios adicionales.
- De forma predeterminada, los cifrados débiles están deshabilitados y las comunicaciones de los clientes están protegidas con SSL. Los algoritmos exactos utilizados para proteger el canal dependen del protocolo de enlace de SSL. Los certificados predeterminados creados en ESXi utilizan el cifrado PKCS#1 SHA-256 con RSA como algoritmo de firmas.
- ESXi utiliza internamente un servicio web Tomcat para admitir el acceso mediante los clientes web. El servicio se modificó para que ejecute solo las funciones que necesita un cliente web para la administración y la supervisión. Como resultado, ESXi no es vulnerable a los problemas de seguridad de Tomcat que se experimentan durante el uso general.
- VMware supervisa todas las alertas de seguridad que pueden afectar la seguridad de ESXi y emite una revisión de seguridad según sea necesario.
- No se instalan servicios no seguros, como FTP y Telnet, y sus puertos están cerrados de forma predeterminada. Dado que hay servicios más seguros que son fáciles de obtener, como SSH y SFTP, evite el uso de los servicios no seguros y opte por alternativas más seguras. Por ejemplo, utilice Telnet con SSL para acceder a los puertos serie virtuales si SSH no está disponible y se debe utilizar Telnet.

  Si debe utilizar servicios no seguros, pero implementó las medidas de seguridad correspondientes para el host, puede abrir puertos de forma explícita para admitir estos servicios.
- Considere usar el arranque seguro UEFI para el sistema ESXi. Consulte Arranque seguro UEFI para hosts ESXi.

Medidas de seguridad adicionales

Tenga en cuenta las siguientes recomendaciones al evaluar la seguridad y la administración de los hosts.

Restricción del acceso

Si habilita el acceso a la interfaz de usuario de la consola directa (DCUI), a ESXi Shell o a SSH, aplique directivas de seguridad de acceso estrictas.

ESXi Shell tiene acceso privilegiado a ciertas partes del host. Proporcione acceso de inicio de sesión a ESXi Shell solo a usuarios de confianza.

Acceso no directo a los hosts administrados

Utilice vSphere Client para administrar los hosts ESXi que administra un sistema vCenter Server. No acceda directamente a los hosts administrados con VMware Host Client y no cambie los hosts administrados de la DCUI.

Si administra hosts con una interfaz o API de scripting, no apunte directamente al host. En su lugar, apunte al sistema vCenter Server que administra el host y especifique el nombre de host.

Usar la DCUI solamente para la solución de problemas

Acceda al host desde la DCUI o ESXi Shell como usuario raíz solo para solucionar problemas. Use uno de los clientes de GUI o una de las CLI o API de VMware para administrar los hosts ESXi. Si utiliza ESXi Shell o SSH, limite las cuentas que tienen acceso y establezca tiempos de espera.

Usar orígenes de VMware solamente para actualizar los componentes de ESXi

El host ejecuta varios paquetes externos para admitir las interfaces de administración o las tareas que se deben realizar. VMware solo admite actualizaciones para estos paquetes que provienen de un origen de VMware. Si utiliza una descarga o una revisión de otro origen, puede comprometer la seguridad o las funciones de la interfaz de administración. Compruebe los sitios de proveedores externos y la base de conocimientos de VMware para consultar las alertas de seguridad.

Nota Siga los avisos de seguridad de VMware en http://www.vmware.com/security/.

Configurar hosts ESXi con Host Profiles

Los perfiles de host permiten establecer configuraciones estándar para los hosts ESXi y automatizar el cumplimiento de estas opciones de configuración. Los perfiles de host permiten controlar varios aspectos de la configuración de hosts, como la memoria, el almacenamiento, las redes, etc.

Se pueden configurar perfiles de host para un host de referencia desde vSphere Client y aplicar el perfil de host a todos los hosts que comparten las características del host de referencia. También se pueden usar perfiles de host para detectar cambios de configuración en los hosts. Consulte el documento *Perfiles de host de vSphere*.

Es posible asociar el perfil de host a un clúster para aplicarlo a todos los hosts de este.

Procedimiento

1 Configure el host de referencia de acuerdo con las especificaciones y cree un perfil de host.

2 Asocie el perfil a un host o un clúster.

3 Aplique el perfil de host del host de referencia a otros hosts o clústeres.

Usar scripts para administrar las opciones de configuración de hosts

En los entornos con muchos hosts, la administración de hosts con scripts resulta más rápida y es menos proclive a errores que la administración de hosts desde vSphere Client.

vSphere incluye varios lenguajes de scripting para la administración de hosts. Consulte la *documentación de vSphere Command-Line* y la *documentación de vSphere API/SDK* para obtener información de referencia y consejos de programación. Consulte las comunidades de VMware para obtener otros consejos sobre la administración generada por script. La documentación sobre el administrador de vSphere se centra en el uso de vSphere Client para realizar la administración.

vSphere PowerCLI

VMware vSphere PowerCLI es una interfaz Windows PowerShell para vSphere API. vSphere PowerCLI incluye cmdlets PowerShell para administrar componentes de vSphere.

vSphere PowerCLI incluye más de 200 cmdlets, un conjunto de scripts de muestra y una biblioteca de funciones para las tareas de administración y automatización. Consulte la *documentación de vSphere PowerCLI*.

vSphere Command-Line Interface (vCLI)

vCLI incluye un conjunto de comandos para administrar las máquinas virtuales y los hosts ESXi. El instalador, que también instala vSphere SDK for Perl, ejecuta sistemas Windows o Linux e instala comandos ESXCLI, comandos `vicfg-` y un conjunto de otros comandos de vCLI. Consulte la *documentación de vSphere Command-Line Interface*.

A partir de vSphere 6.0, también es posible usar una de las interfaces de scripting en vCloud Suite SDK, como vCloud Suite SDK for Python.

Procedimiento

1 Cree una función personalizada con privilegios limitados.

Por ejemplo, considere crear una función que contenga un conjunto de privilegios para administrar hosts, pero que no incluya privilegios para administrar máquinas virtuales, almacenamiento o redes. Si el script que desea usar solamente extrae información, puede crear una función con privilegios de solo lectura para el host.

2 En vSphere Client, cree una cuenta de servicio y asigne la función personalizada a esa cuenta.

Puede crear varias funciones personalizadas con diferentes niveles de acceso si desea que el acceso a determinados hosts sea bastante limitado.

3 Escriba scripts para comprobar o modificar parámetros, y ejecute esos scripts.

Por ejemplo, puede comprobar o establecer el tiempo de espera interactivo del shell de un host de la siguiente manera:

<table>
<tr><th>Lenguaje</th><th>Comandos</th></tr>
<tr><td>vCLI (ESXCLI)</td><td><pre>esxcli <conn_options> system settings advanced get /
UserVars/ESXiShellTimeOut</pre><pre>esxcli --formatter=csv --format-param=fields="Path,Int
Value"
system settings advanced list | grep /UserVars/
ESXiShellTimeOut</pre></td></tr>
<tr><td>PowerCLI</td><td><pre>#List UserVars.ESXiShellInteractiveTimeOut for each host
Get-VMHost | Select Name,
 @{N="UserVars.ESXiShellInteractiveTimeOut";E={$_
| Get-AdvancedSetting -Name
UserVars.ESXiShellInteractiveTimeOut
| Select -ExpandProperty Value}}

Set UserVars.ESXiShellTimeOut to 900 on all hosts
Get-VMHost
| Foreach { Get-AdvancedSetting -Entity $_
-Name UserVars.ESXiShellInteractiveTimeOut | Set-
AdvancedSetting -Value 900 }</pre></td></tr>
</table>

4 En entornos grandes, cree funciones con diferentes privilegios de acceso y hosts de grupos en carpetas según las tareas que desee realizar. Posteriormente, puede ejecutar scripts en diferentes carpetas desde diferentes cuentas de servicio.

5 Verifique que se hayan producido cambios después de ejecutar el comando.

Bloqueo de cuenta y contraseñas ESXi

Para los hosts ESXi, debe utilizar una contraseña con requisitos predefinidos. Puede cambiar el requisito de longitud requerida y clases de caracteres o permitir frases de contraseña si utiliza la opción avanzada `Security.PasswordQualityControl`. También puede establecer

el número de contraseñas para recordar para cada usuario mediante la opción avanzada `Security.PasswordHistory`.

Nota Los requisitos predeterminados para las contraseñas de ESXi pueden cambiar de una versión a otra. Puede comprobar las restricciones predeterminadas para la contraseña y modificarlas con la opción avanzada `Security.PasswordQualityControl`.

Contraseñas de ESXi

ESXi aplica requisitos de contraseña para el acceso desde la interfaz de usuario de la consola directa, ESXi Shell, SSH o VMware Host Client.

- De manera predeterminada, cuando cree la contraseña deberá incluir una combinación de cuatro clases de caracteres: letras en minúscula, letras en mayúscula, números y caracteres especiales, como el guion bajo o el guion.
- De forma predeterminada, la longitud de la contraseña debe tener más de 7 caracteres y menos de 40.
- Las contraseñas no pueden contener una palabra de diccionario o parte de una palabra de diccionario.

Nota Un carácter en mayúscula al inicio de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan. Un número al final de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan.

Ejemplos de contraseñas de ESXi

A continuación se indican posibles contraseñas en caso de configurar la opción de la siguiente manera.

```
retry=3 min=disabled,disabled,disabled,7,7
```

Con esta opción, se solicita al usuario hasta tres veces (retry=3) una contraseña nueva si no es lo suficientemente segura o si la contraseña no se introdujo correctamente dos veces. No se permiten las contraseñas que tienen una o dos clases de caracteres ni las frases de contraseña, ya que los primeros tres elementos están deshabilitados. Las contraseñas de tres y cuatro clases de caracteres requieren siete caracteres. Consulte la página del manual de `pam_passwdqc` para obtener más información sobre otras opciones, como `max` y `passphrase`, entre otras.

Con esta configuración, se permiten las siguientes contraseñas.

- xQaTEhb!: contiene ocho caracteres de tres clases.
- xQaT3#A: contiene siete caracteres de cuatro clases.

Las siguientes contraseñas posibles no cumplen con los requisitos.

- Xqat3hi: comienza con un carácter en mayúscula, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.

- xQaTEh2: termina con un número, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.

Frase de contraseña de ESXi

En lugar de una contraseña, también puede utilizar una frase de contraseña. Sin embargo, las frases de contraseña están deshabilitadas de forma predeterminada. Puede cambiar este valor predeterminado u otros valores de configuración mediante la opción avanzada `Security.PasswordQualityControl` de vSphere Client.

Por ejemplo, puede cambiar la opción por la siguiente.

```
retry=3 min=disabled,disabled,16,7,7
```

Este ejemplo permite frases de contraseña de al menos 16 caracteres y un mínimo de 3 palabras separadas por espacios.

En el caso de los hosts heredados, todavía se puede cambiar el archivo `/etc/pamd/passwd`, pero no se podrá hacer en las próximas versiones. En su lugar, utilice la opción avanzada `Security.PasswordQualityControl`.

Modificar las restricciones predeterminadas de contraseña

Puede cambiar la restricción predeterminada de contraseñas y frases de contraseña con la opción avanzada `Security.PasswordQualityControl` (Control de calidad de contraseña de seguridad) del host ESXi. Consulte la documentación *Administrar vCenter Server y hosts* para obtener información sobre la configuración de las opciones avanzadas de ESXi.

Puede cambiar el valor predeterminado, por ejemplo, para requerir un mínimo de 15 caracteres y una cantidad mínima de cuatro palabras (`passphrase=4`) de la siguiente manera:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

Para obtener más información, consulte la página del manual de `pam_passwdqc`.

Nota Aún no se han probado todas las combinaciones posibles de opciones de contraseña. Después de cambiar la configuración de contraseña predeterminada, realice una prueba adicional.

Comportamiento del bloqueo de cuentas de ESXi

Se admite el bloqueo de cuentas para el acceso a través de SSH y vSphere Web Services SDK. La interfaz de la consola directa (DCUI) y ESXi Shell no admiten el bloqueo de cuentas. De forma predeterminada, se permite un máximo de cinco intentos con errores antes de que la cuenta se bloquee. De forma predeterminada, la cuenta se desbloquea después de 15 minutos.

Configurar el comportamiento de inicio de sesión

Puede configurar el comportamiento de inicio de sesión del host ESXi con las siguientes opciones avanzadas:

- `Security.AccountLockFailures`. Cantidad máxima de intentos de inicio de sesión con errores antes de que la cuenta de un usuario se bloquee. Cero deshabilita el bloqueo de cuentas.
- `Security.AccountUnlockTime`. Cantidad de segundos en los que el usuario queda bloqueado.
- `Security.PasswordHistory`. Cantidad de contraseñas que se deben recordar para cada usuario. Si se especifica cero, se deshabilita el historial de contraseñas.

Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la configuración de las opciones avanzadas de ESXi.

Seguridad de SSH

ESXi Shell y las interfases SSH están deshabilitados de forma predeterminada. Mantenga estas interfaces deshabilitadas a menos que esté realizando actividades de solución de problemas o de soporte. Para las actividades cotidianas, utilice la vSphere Client, donde la actividad está sujeta al control de acceso basado en roles y a métodos de control de acceso modernos.

La configuración de SSH en ESXi utiliza las siguientes opciones:

Protocolo SSH versión 1 deshabilitado

VMware no admite el protocolo SSH versión 1 y usa el protocolo versión 2 de forma exclusiva. La versión 2 elimina determinados problemas de seguridad que tiene la versión 1 y ofrece una forma segura de comunicarse con la interfaz de administración.

Intensidad de cifrado mejorada

SSH admite solo cifrados AES de 256 y 128 bits para las conexiones.

Está configuración está diseñada para proporcionar una protección sólida de los datos que se transmiten a la interfaz de administración a través de SSH. Esta configuración no se puede cambiar.

Claves SSH de ESXi

Las claves SSH pueden restringir, controlar y proteger el acceso a un host ESXi. Una clave SSH puede permitir que un usuario de confianza o un script inicien sesión en un host sin especificar una contraseña.

Puede copiar la clave SSH en el host mediante el comando de CLI `vifs` vSphere. Consulte *Introducción a vSphere Command-Line Interface* para obtener información sobre cómo instalar y utilizar el conjunto de comandos de CLI de vSphere. También puede utilizar el método PUT de HTTPS para copiar la clave SSK en el host.

En lugar de generar claves de forma externa y cargarlas, es posible crearlas en el host ESXi y descargarlas. Consulte el artículo de base de conocimientos de VMware en http://kb.vmware.com/kb/1002866.

Habilitar SSH y agregar claves SSH al host presenta riesgos innatos. Compare el riesgo potencial de exponer un nombre de usuario y una contraseña contra el riesgo de intromisión de un usuario que tenga una clave confiable.

Nota En ESXi 5.0 y versiones anteriores, un usuario con una clave SSH puede acceder al host incluso si este se encuentra en modo de bloqueo. A partir de ESXi 5.1, un usuario con una clave SSH ya no puede acceder a un host en modo de bloqueo.

Cargar una clave SSH mediante un comando vifs

Si decide que desea utilizar claves autorizadas para iniciar sesión en un host con SSH, puede cargarlas con un comando `vifs`.

Nota Debido a que las claves autorizadas permiten el acceso SSH sin requerir autenticación de usuario, evalúe detenidamente si desea usar claves SSH en el entorno.

Las claves autorizadas permiten autenticar el acceso remoto a un host. Cuando los usuarios o scripts intentan acceder a un host con SSH, la clave proporciona la autenticación sin solicitar una contraseña. Las claves autorizadas permiten automatizar la autenticación, lo cual resulta útil para escribir scripts que realizan tareas de rutina.

Puede cargar en un host los siguientes tipos de claves SSH.

- Archivos de claves autorizadas para el usuario raíz
- Clave de RSA
- Clave pública de RSA

A partir de la versión vSphere 6.0 Update 2, las claves DSS/DSA ya no son compatibles.

Importante No modifique el archivo `/etc/ssh/sshd_config`. Si lo hace, realice un cambio sobre el cual el daemon del host (`hostd`) no sepa nada.

Procedimiento

- En la línea de comandos o en un servidor de administración, use el comando `vifs` para cargar la clave SSH en la ubicación correcta en el host ESXi.

```
vifs --server hostname --username username --put filename /host/ssh_host_dsa_key_pub
```

Tipo de clave	Ubicación
Archivos de claves autorizadas para el usuario raíz	`/host/ssh_root_authorized_keys` Debe tener privilegios de administrador completos para poder cargar el archivo.
Claves RSA	`/host/ssh_host_rsa_key`
Claves públicas RSA	`/host/ssh_host_rsa_key_pub`

Cargar una clave SSH mediante el método PUT de HTTPS

Puede utilizar claves autorizadas para iniciar sesión en un host con SSH. Puede cargar las claves autorizadas mediante el método PUT de HTTPS.

Las claves autorizadas permiten autenticar el acceso remoto a un host. Cuando los usuarios o scripts intentan acceder a un host con SSH, la clave proporciona la autenticación sin solicitar una contraseña. Las claves autorizadas permiten automatizar la autenticación, lo cual resulta útil para escribir scripts que realizan tareas de rutina.

Puede cargar en un host los siguientes tipos de claves SSH mediante el método PUT de HTTPS:

- Archivo de claves autorizadas para el usuario raíz
- Clave DSA
- Clave pública de DSA
- Clave de RSA
- Clave pública de RSA

Importante No modifique el archivo `/etc/ssh/sshd_config`.

Procedimiento

1 En la aplicación de carga, abra el archivo de claves.

2 Publique el archivo en las siguientes ubicaciones.

Tipo de clave	Ubicación
Archivos de claves autorizadas para el usuario raíz	`https://`*`hostname_or_IP_address`*`/host/ssh_root_authorized_keys` Debe tener privilegios completos de administrador sobre el host para poder cargar el archivo.
Claves DSA	`https://`*`hostname_or_IP_address`*`/host/ssh_host_dsa_key`
Claves públicas DSA	`https://`*`hostname_or_IP_address`*`/host/ssh_host_dsa_key_pub`
Claves RSA	`https://`*`hostname_or_IP_address`*`/host/ssh_host_rsa_key`
Claves públicas RSA	`https://`*`hostname_or_IP_address`*`/host/ssh_host_rsa_key_pub`

Dispositivos PCI/PCIe y ESXi

El uso de VMware DirectPath I/O para establecer el acceso directo de un dispositivo PCI o PCIe a una máquina virtual representa una vulnerabilidad potencial de la seguridad. La vulnerabilidad se puede activar debido a que un código malintencionado o defectuoso (como un controlador de dispositivo) se ejecuta en modo privilegiado en el sistema operativo invitado. Actualmente, el hardware y el firmware estándar del sector no admiten la contención de errores para proteger los hosts ESXi de esta vulnerabilidad.

Use el acceso directo PCI o PCIe a una máquina virtual solo si una entidad de confianza posee y administra la máquina virtual. Es necesario tener la certeza de que esta entidad no intentará bloquear o aprovechar el host de la máquina virtual.

Es posible que el host quede comprometido de una de las siguientes maneras.

- El sistema operativo invitado puede generar un error de PCI o PCIe irrecuperable. Un error de ese tipo no daña los datos, pero puede bloquear el host ESXi. Esos errores pueden ser resultado de errores o incompatibilidades en los dispositivos de hardware para los que se establecen accesos directos. Otros motivos para los errores incluyen problemas con los controladores en el sistema operativo invitado.
- El sistema operativo invitado puede generar una operación de acceso directo a memoria (DMA) que provoque un error de página IOMMU en el host ESXi. Esta operación podría ser el resultado de una operación de DMA cuyo objetivo fuera una dirección fuera de la memoria de la máquina virtual. En algunas máquinas, el firmware del host configura los errores de IOMMU para que notifiquen un error irrecuperable a través de una interrupción no enmascarable (NMI). Este error irrecuperable hace que el host ESXi se bloquee. La causa de esto pueden ser problemas con los controladores en el sistema operativo invitado.
- Si el sistema operativo en el host ESXi no utiliza la reasignación de interrupciones, es posible que el sistema operativo invitado inyecte una interrupción falsa en el host ESXi en cualquier vector. Actualmente, ESXi utiliza la reasignación de interrupciones en las plataformas Intel donde se encuentra disponible. La asignación de interrupciones forma parte del conjunto de características de Intel VT-d. ESXi no utiliza la asignación de interrupciones en las plataformas AMD. Una interrupción falsa puede bloquear el host ESXi. En teoría, es posible que existan otras formas de aprovechar estas interrupciones falsas.

Deshabilitar el explorador de objetos administrados

El explorador de objetos administrados (Managed Object Browser, MOB) permite explorar el modelo de objetos VMkernel. Sin embargo, los atacantes pueden utilizar esta interfaz para realizar acciones o cambios maliciosos en la configuración porque se puede cambiar la configuración del host desde el MOB. Utilice el MOB únicamente para depurar y asegúrese de que esté deshabilitado en los sistemas de producción.

A partir de vSphere 6.0, el MOB se encuentra deshabilitado de forma predeterminada. Sin embargo, es necesario utilizar el MOB para ciertas tareas, por ejemplo, para extraer un certificado antiguo de un sistema. Puede habilitar o deshabilitar el MOB de la siguiente manera.

Procedimiento

1. Desplácese hasta el host en el inventario de vSphere Client.
2. Haga clic en **Configurar**.
3. En Sistema, haga clic en **Configuración avanzada del sistema**.

4 Compruebe el valor de **Config.HostAgent.plugins.solo.enableMob** y haga clic en **Editar** para cambiarlo según corresponda.

   No utilice `vim-cmd` desde ESXi Shell.

Recomendaciones de seguridad para redes de ESXi

El aislamiento del tráfico de red es fundamental para proteger el entorno de ESXi. Las distintas redes requieren diferente acceso y nivel de aislamiento.

El host ESXi usa varias redes. Emplee las medidas de seguridad que correspondan para cada red y aísle el tráfico de aplicaciones y funciones específicas. Por ejemplo, asegúrese de que el tráfico de VMware vSphere® vMotion® no pase por redes en las que haya máquinas virtuales. El aislamiento impide las intromisiones. Además, por motivos de rendimiento, también se recomienda usar redes separadas.

- Las redes de infraestructura de vSphere se usan para funciones como vSphere vMotion, VMware vSphere Fault Tolerance, VMware vSAN y almacenamiento. Aísle estas redes según sus funciones específicas. Generalmente, no es necesario dirigir estas redes fuera de un rack de servidor físico único.
- Una red de administración aísla los distintos tráficos (tráfico de clientes, de la interfaz de la línea de comandos (CLI) o de la API, y del software de terceros) de otros tráficos. Esta red debe estar accesible únicamente para los administradores de sistemas, redes y seguridad. Use jump box o Virtual Private Network (VPN) para proteger el acceso a la red de administración. Controle estrictamente el acceso dentro de esta red.
- El tráfico de las máquinas virtuales puede transmitirse por medio de una red o de muchas. Puede optimizar el aislamiento de las máquinas virtuales mediante soluciones de firewall virtuales que establezcan reglas de firewall en la controladora de red virtual. Esta configuración se envía junto con una máquina virtual cuando esta se migra de un host a otro dentro del entorno de vSphere.

Modificar la configuración del proxy web de ESXi

Al modificar la configuración del proxy web, hay varias directrices de seguridad del usuario y del cifrado que se deben tener en cuenta.

Nota Reinicie el proceso del host después de realizar cualquier cambio en los directorios o los mecanismos de autenticación del host.

- No configure certificados que utilicen una contraseña o frases de contraseña. ESXi no es compatible con proxies web que utilizan contraseñas o frases de contraseña, llamadas también claves cifradas. Si se configura un proxy web que requiere una contraseña o una frase de contraseña, los procesos de ESXi no podrán iniciarse correctamente.

- Para que resulte compatible el cifrado de los nombres de usuario, las contraseñas y los paquetes, SSL se habilita de forma predeterminada en las conexiones de vSphere Web Services SDK. Si se desea configurar estas conexiones de modo que no cifren las transmisiones, deshabilite SSL en la conexión de vSphere Web Services SDK. Para ello, cambie la conexión de HTTPS a HTTP.

  Considere deshabilitar SSL solo si creó un entorno de plena confianza para estos clientes, donde los firewalls estén establecidos y las transmisiones desde y hacia el host estén aisladas por completo. Si se deshabilita SSL, se puede mejorar el rendimiento debido a que se evita la sobrecarga requerida para el cifrado.

- Para evitar la utilización incorrecta de los servicios de ESXi, se puede acceder a la mayoría de los servicios internos de ESXi únicamente mediante el puerto 443, el puerto utilizado para la transmisión de HTTPS. El puerto 443 funciona como un proxy inverso de ESXi. Se puede ver la lista de servicios en ESXi a través de la página principal de HTTP, pero no se puede acceder directamente a los servicios de adaptadores de almacenamiento sin la debida autorización.

  Se puede cambiar esta configuración de modo que los servicios individuales sean accesibles directamente a través de las conexiones de HTTP. No realice este cambio, a menos que utilice ESXi en un entorno de plena confianza.

- Al actualizar el entorno, el certificado permanece en su ubicación.

Consideraciones de seguridad de vSphere Auto Deploy

Cuando utilice vSphere Auto Deploy, preste especial atención a la seguridad de redes, a la seguridad de la imagen de arranque y a la posible exposición de la contraseña en los perfiles de host para proteger su entorno.

Seguridad de redes

Asegure su red igual que si se tratara de cualquier otro método de implementación basado en PXE. vSphere Auto Deploy transfiere datos por SSL para evitar interferencias accidentales e intromisiones. Sin embargo, la autenticidad del cliente o del servidor Auto Deploy no se comprueba durante un arranque PXE.

Puede reducir ampliamente el riesgo de seguridad de Auto Deploy aislando por completo la red donde se utiliza Auto Deploy.

Imagen de arranque y seguridad de perfil de host

La imagen de arranque que descarga el servidor vSphere Auto Deploy en una máquina puede tener los siguientes componentes.

- Los paquetes de VIB que componen el perfil de imagen se incluyen siempre en la imagen de arranque.

- El perfil de host y la personalización del host se incluyen en la imagen de arranque si las reglas de Auto Deploy se configuran para aprovisionar el host con un perfil o una personalización del host.
  - La contraseña de administrador (raíz) y las contraseñas de usuario que se incluyen en el perfil de host y en la personalización de host están cifradas con hash SHA-512.
  - Cualquier otra contraseña asociada a los perfiles quedará excluida. Si configura Active Directory utilizando perfiles de host, las contraseñas no poseen protección.

    Utilice vSphere Authentication Proxy para evitar la exposición de las contraseñas de Active Directory. Si configura Active Directory utilizando perfiles de host, las contraseñas no están protegidas.
- El certificado y la clave SSL públicas y privadas del host se incluyen en la imagen de arranque.

Acceso de control para herramientas de supervisión de hardware basadas en CIM

El sistema del modelo de información común (CIM) proporciona una interfaz que habilita la administración en el nivel del hardware desde aplicaciones remotas que usan un conjunto de interfaces de programación de aplicaciones (API) estándar. Para garantizar que la interfaz de CIM sea segura, proporcione únicamente el acceso mínimo y necesario a estas aplicaciones remotas. Si aprovisiona una aplicación remota con una cuenta raíz o de administrador y si la aplicación está comprometida, puede comprometerse el entorno virtual.

CIM es un estándar abierto que establece un marco para la supervisión de recursos de hardware sin agente basada en estándares para hosts ESXi. Este marco consta de un administrador de objetos CIM, a menudo llamado agente CIM, y un conjunto de proveedores CIM.

Los proveedores de CIM admiten acceso de administración para controladores de dispositivos y hardware subyacente. Los proveedores de hardware, incluidos los fabricantes de servidores y los proveedores de dispositivos de hardware, pueden escribir proveedores que supervisen y administren sus dispositivos. VMware escribe proveedores que supervisan hardware de servidor, infraestructura de almacenamiento de ESXi y recursos específicos de virtualización. Estos proveedores se ejecutan dentro del host ESXi. Son livianos y se centran en tareas específicas de administración. El agente CIM toma información de todos los proveedores de CIM y usa API estándar para presentar la información al mundo exterior. La API más común es WS-MAN.

No proporcione credenciales de raíz a aplicaciones remotas que accedan a la interfaz de CIM. En su lugar, cree una cuenta de usuario de vSphere con menos privilegios para estas aplicaciones y utilice la función de ticket de API de VIM para emitir un valor de sessionId (denominado "ticket") para esta cuenta de usuario con menos privilegios para autenticarse en CIM. Si se le concede un permiso a la cuenta para obtener tickets de CIM, la API de VIM puede proporcionar el ticket a CIM. A continuación, estos tickets se proporcionan como la contraseña y el identificador de usuario a cualquier llamada API de CIM-XML. Consulte el método `AcquireCimServicesTicket()` para obtener más información.

El servicio CIM se inicia cuando se instala un CIM VIB de terceros (por ejemplo, cuando se ejecuta el comando `esxcli software vib install -n VIBname`).

Si se debe habilitar el servicio CIM manualmente, ejecute el siguiente comando:

```
esxcli system wbem set -e true
```

Si es necesario, puede deshabilitar wsman (servicio WSManagement) para que se ejecute solamente el servicio CIM:

```
esxcli system wbem set -W false
```

Para confirmar que se deshabilitó wsman, ejecute el siguiente comando:

```
esxcli system wbem get
…
WSManagement PID: 0
WSManagement Service: false
```

Para obtener más información acerca de los comandos de ESXCLI, consulte la *documentación de la interfaz de línea de comandos de vSphere*. Para obtener más información sobre cómo habilitar el servicio CIM, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/kb/1025757.

Procedimiento

1 Cree una cuenta de usuario no raíz de vSphere para las aplicaciones de CIM.

   Consulte el tema sobre cómo agregar usuarios de vCenter Single Sign-On en la *Guía de administración de Platform Services Controller*. El privilegio de vSphere necesario para la cuenta de usuario es **Host.CIM.Interacción**.

2 Utilice el SDK de vSphere API que desee para autenticar la cuenta de usuario en vCenter Server. A continuación, realice una llamada a `AcquireCimServicesTicket()` para devolver un ticket con el fin de autenticarse con ESXi como una cuenta de nivel de administrador mediante las API del puerto 5989 de CIM-XML o del puerto 433 de WS-Man.

   Consulte la documentación de *Referencia de VMware vSphere API* para obtener más información.

3 Renueve el ticket cada dos minutos según sea necesario.

Administrar certificados para hosts ESXi

En vSphere 6.0 y versiones posteriores, VMware Certificate Authority (VMCA) aprovisiona a cada host nuevo de ESXi con un certificado firmado cuya entidad de certificación raíz de forma predeterminada es VMCA. El aprovisionamiento ocurre cuando se agrega el host a vCenter Server explícitamente, o bien como parte de la instalación o la actualización a ESXi 6.0 o una versión posterior.

Puede ver y administrar certificados de ESXi desde vSphere Client y con la API de `vim.CertificateManager` en vSphere Web Services SDK. No puede ver ni administrar los certificados de ESXi por medio de las CLI de administración de certificados que están disponibles para administrar certificados de vCenter Server.

Certificados en vSphere 5.5 y en vSphere 6.x

Cuando ESXi y vCenter Server se comunican, utilizan TLS/SSL para casi todo el tráfico de administración.

En vSphere 5.5 y versiones anteriores, los extremos de TLS/SSL están protegidos únicamente por una combinación de nombre de usuario, contraseña y huella digital. Los usuarios pueden reemplazar los correspondientes certificados autofirmados por sus propios certificados. Consulte el centro de documentación de vSphere 5.5.

En vSphere 6.0 y versiones posteriores, vCenter Server admite los siguientes modos de certificación para los hosts ESXi.

Tabla 3-1. Modos de certificación para hosts ESXi

Modo de certificación	Descripción
VMware Certificate Authority (predeterminada)	Utilice este modo si VMCA aprovisiona a todos los hosts ESXi, ya sea como entidad de certificación intermedia o de nivel superior. VMCA aprovisiona de forma predeterminada a los hosts ESXi con certificados. En este modo, es posible actualizar y renovar los certificados desde vSphere Client.
Entidad de certificación personalizada	Utilice este modo si desea utilizar solamente certificados personalizados que estén firmados por una entidad de certificación externa o empresarial. En este modo, usted es responsable de administrar los certificados. No puede actualizar ni renovar los certificados desde vSphere Client. **Nota** A menos que cambie el modo de certificación al modo Entidad de certificación personalizada, VMCA podrá reemplazar los certificados personalizados, por ejemplo, al seleccionar **Renovar** en vSphere Client.
Modo de huella digital	vSphere 5.5 usaba el modo de huella digital, el cual todavía está disponible como opción de reserva para vSphere 6.x. En este modo, vCenter Server verifica que el certificado tenga el formato correcto, pero no verifica la validez del certificado. Se aceptan incluso los certificados que caducaron. No utilice este modo a menos que detecte problemas con uno de los otros dos modos y no pueda solucionarlos. Algunos servicios de vCenter 6.x y de versiones posteriores pueden funcionar de forma incorrecta en el modo de huella digital.

Caducidad de los certificados

A partir de vSphere 6.0, puede ver información sobre la caducidad de los certificados firmados por VMCA o por una entidad de certificación externa en vSphere Client. Puede ver la información de todos los hosts administrados por vCenter Server o de hosts individuales. Una alarma de color amarillo se enciende si el certificado se encuentra en estado **Por caducar en breve** (dentro de menos de ocho meses). Una alarma de color rojo se enciende si el certificado se encuentra en estado **Caducidad inminente** (dentro de menos de dos meses).

Aprovisionar ESXi y VMCA

Cuando inicia un host ESXi desde los medios de instalación, el host en principio tiene un certificado autogenerado. Cuando se agrega el host al sistema vCenter Server, se le aprovisiona un certificado firmado por VMCA como entidad de certificación raíz.

El proceso es similar para los hosts aprovisionados con Auto Deploy. No obstante, dado que esos hosts no almacenan ningún estado, el servidor Auto Deploy almacena el certificado firmado en su almacén local de certificados. El certificado se vuelve a utilizar en los arranques subsiguientes de los hosts ESXi. Un servidor Auto Deploy forma parte de cualquier implementación integrada o sistema de vCenter Server.

Si VMCA no está disponible cuando un host Auto Deploy se inicia por primera vez, el host primero intenta conectarse. Si el host no puede conectarse, realiza un ciclo de apagado y reinicio hasta que VMCA está disponible y el host puede aprovisionarse con un certificado firmado.

Privilegios necesarios para la administración de certificados de ESXi

Para administrar certificados de los hosts ESXi, se debe tener el privilegio **Certificados.Administrar certificados**. Este privilegio se puede establecer desde vSphere Client.

Cambios en el nombre de host y la dirección IP

En vSphere 6.0 y versiones posteriores, un cambio en el nombre de host o la dirección IP podría afectar si vCenter Server considera que un certificado de host es válido o no. El modo en que se agregó el host a vCenter Server puede hacer que sea necesario una intervención manual. Por intervención manual se entiende que se debe volver a conectar el host, o bien se lo debe quitar de vCenter Server y volver a agregar.

Tabla 3-2. Cuando el nombre de host o la dirección IP se deben cambiar de forma manual

Se agregó un host a vCenter Server mediante...	Cambios en el nombre de host	Cambios en la dirección IP
Nombre de host	Problema de conectividad de vCenter Server. Se necesita una intervención manual.	No se debe realizar ninguna acción.
Dirección IP	No se debe realizar ninguna acción.	Problema de conectividad de vCenter Server. Se necesita una intervención manual.

Administración de certificados de ESXi (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vkuyp3rf/uiConfId/49694343/)

Certificados y actualizaciones de hosts

Si actualiza un host ESXi a ESXi 6.5 o una versión posterior, el proceso de actualización reemplaza los certificados autofirmados (huella digital) por certificados firmados por VMCA. Si el host ESXi utiliza certificados personalizados, el proceso de actualización conserva esos certificados aun si caducaron o no son válidos.

El flujo de trabajo recomendado para actualizar depende de los certificados actuales.

Host aprovisionado con certificados de huellas digitales

Si el host actualmente usa certificados de huellas digitales, se le asignan certificados de VMCA de manera automática como parte del proceso de actualización.

Nota No se pueden aprovisionar hosts heredados con certificados de VMCA. Debe actualizar estos hosts a ESXi 6.5 o una versión posterior.

Host aprovisionado con certificados personalizados

Si el host se aprovisiona con certificados personalizados (por lo general, certificados externos firmados por entidades de certificación), esos certificados permanecen en su lugar durante la actualización. Cambie el modo de certificado a **Personalizado** para asegurarse de no reemplazar accidentalmente los certificados durante una actualización de certificados posterior.

Nota Si el entorno se encuentra en modo VMCA y se actualizan los certificados desde vSphere Client, todos los certificados existentes se reemplazan por certificados firmados por VMCA.

Posteriormente, vCenter Server supervisa los certificados y muestra información, como la caducidad del certificado, en vSphere Client.

Hosts aprovisionados con Auto Deploy

Siempre se asignan nuevos certificados a los hosts que aprovisiona Auto Deploy cuando se arrancan por primera vez con el software ESXi 6.5 o una versión posterior. Al actualizar un host aprovisionado por Auto Deploy, el servidor Auto Deploy genera una solicitud de firma del certificado (CSR) para el host y la envía a VMCA. VMCA almacena el certificado firmado para el host. Cuando el servidor Auto Deploy aprovisiona el host, este recupera el certificado de VMCA y lo incluye en el proceso de aprovisionamiento.

Puede utilizar Auto Deploy con certificados personalizados.

Consulte Usar certificados personalizados con Auto Deploy.

Flujos de trabajo de cambio de modo de certificado

A partir de vSphere 6.0, los hosts ESXi están aprovisionados de forma predeterminada con certificados de VMCA. En lugar de eso, es posible usar el modo de certificación personalizada o, con fines de depuración, el modo de huella digital heredado. En la mayoría de los casos, los cambios de modo son disruptivos e innecesarios. Si el cambio de modo es necesario, revise el posible impacto que puede provocar antes de realizarlo.

En vSphere 6.0 y versiones posteriores, vCenter Server admite los siguientes modos de certificación para los hosts ESXi.

Modo de certificación	Descripción
VMware Certificate Authority (predeterminada)	De forma predeterminada, se usa VMware Certificate Authority para los certificados de hosts ESXi. VMCA es la entidad de certificación raíz predeterminada, pero se puede configurar como la entidad de certificación intermedia de otra entidad. En este modo, los usuarios pueden administrar los certificados desde vSphere Client. También se usa si VMCA es un certificado subordinado.
Entidad de certificación personalizada	Algunos clientes pueden preferir administrar su propia entidad de certificación externa. En este modo, los clientes son responsables de administrar los certificados y no pueden hacerlo desde vSphere Client.
Modo de huella digital	vSphere 5.5 usaba el modo de huella digital, el cual todavía está disponible como opción de reserva para vSphere 6.0. No utilice este modo a menos que encuentre problemas que no puede resolver con uno de los otros dos modos. Algunos servicios de vCenter 6.0 y de versiones posteriores pueden funcionar de forma incorrecta en el modo de huella digital.

Usar certificados ESXi personalizados

Si la directiva de la empresa exige que se use una entidad de certificación raíz distinta de VMCA, puede cambiar el modo de certificación en el entorno después de una minuciosa planificación. El siguiente es el flujo de trabajo.

1 Obtenga los certificados que desea utilizar.

2 Coloque el host o los hosts en modo de mantenimiento y desconéctelos de vCenter Server.

3 Agregue el certificado raíz de la entidad de certificación personalizada a VECS.

4 Implemente los certificados de la entidad de certificación personalizada en cada host y reinicie los servicios de dicho host.

5 Cambie al modo de entidad de certificación personalizada. Consulte Cambiar el modo de certificado.

6 Conecte el host o los hosts al sistema de vCenter Server.

Cambiar del modo de entidad de certificación personalizada al modo VMCA

Si está usando el modo de entidad de certificación personalizada y cree que el modo VMCA puede funcionar mejor en su entorno, puede realizar el cambio de modo después de una minuciosa planificación. El siguiente es el flujo de trabajo.

1 Quite todos los hosts del sistema vCenter Server.

2 En el sistema vCenter Server, elimine de VECS el certificado raíz de la entidad de certificación externa.

3 Cambie al modo VMCA. Consulte Cambiar el modo de certificado.

4 Agregue los hosts al sistema vCenter Server.

Nota Si sigue otro flujo de trabajo para este cambio de modo, se puede generar un comportamiento impredecible.

Conservar los certificados del modo de huella digital durante la actualización

El cambio del modo VMCA al modo de huella digital puede resultar necesario si se producen problemas con los certificados de VMCA. En el modo de huella digital, el sistema vCenter Server comprueba que exista un solo certificado y que su formato sea el correcto, pero no comprueba si el certificado es válido. Consulte Cambiar el modo de certificado para obtener instrucciones.

Cambiar del modo de huella digital al modo VMCA

Si usa el modo de huella digital y desea comenzar a usar certificados firmados por VMCA, debe planificar un poco el cambio. El siguiente es el flujo de trabajo.

1 Quite todos los hosts del sistema vCenter Server.

2 Cambie al modo de certificación de VMCA. Consulte Cambiar el modo de certificado.

3 Agregue los hosts al sistema vCenter Server.

Nota Si sigue otro flujo de trabajo para este cambio de modo, se puede generar un comportamiento impredecible.

Cambiar del modo de entidad de certificación personalizada al modo de huella digital

Si experimenta problemas con la entidad de certificación personalizada, considere cambiar temporalmente al modo de huella digital. El cambio se ejecutará sin problemas si sigue las instrucciones detalladas en Cambiar el modo de certificado. Después de cambiar el modo, el sistema vCenter Server comprueba solamente el formato del certificado y ya no comprueba la validez del certificado.

Cambiar del modo de huella digital al modo de entidad de certificación personalizada

Si establece el entorno en el modo de huella digital durante la solución de problemas y desea comenzar a usar el modo de entidad de certificación personalizada, primero debe generar los certificados necesarios. El siguiente es el flujo de trabajo.

1 Quite todos los hosts del sistema vCenter Server.

2 Agregue el certificado raíz de la entidad de certificación personalizada al almacén TRUSTED_ROOTS de VECS en el sistema vCenter Server. Consulte Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados).

3 En cada host ESXi:

   a Implemente la clave y el certificado de la entidad de certificación personalizada.

   b Reinicie los servicios del host.

4 Cambie al modo personalizado. Consulte Cambiar el modo de certificado.

5 Agregue los hosts al sistema vCenter Server.

Configuración predeterminada de certificados ESXi

Cuando se agrega un host al sistema vCenter Server, vCenter Server envía una solicitud de firma de certificado (CSR) para el host en VMCA. Muchos de los valores predeterminados son adecuados para diversas situaciones, pero la información específica de la empresa puede cambiarse.

Puede cambiar varios de los valores predeterminados mediante vSphere Client. Considere cambiar la información de la organización y ubicación. Consulte Cambiar configuración predeterminada de certificados.

Tabla 3-3. Configuración de CSR ESXi

Parámetro	Valor predeterminado	Opción avanzada
Tamaño de clave	2048	N.A.
Algoritmo de clave	RSA	N.A.
Algoritmo de firma de certificado	sha256WithRSAEncryption	N.A.
Nombre común	Nombre del host si este se agregó a vCenter Server por nombre de host. Dirección IP del host si este se agregó a vCenter Server por dirección IP.	N.A.
País	EE. UU.	vpxd.certmgmt.certs.cn.country
Dirección de correo electrónico	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
Localidad (Ciudad)	Palo Alto	vpxd.certmgmt.certs.cn.localityName
Nombre de unidad de organización	Ingeniería de VMware	vpxd.certmgmt.certs.cn.organizationalUnitName
Nombre de organización	VMware	vpxd.certmgmt.certs.cn.organizationName
Estado o provincia	California	vpxd.certmgmt.certs.cn.state
Cantidad de días en que el certificado es válido.	1825	vpxd.certmgmt.certs.daysValid

Tabla 3-3. Configuración de CSR ESXi (continuación)

Parámetro	Valor predeterminado	Opción avanzada
Umbral estricto para la caducidad de los certificados. vCenter Server activa una alarma roja cuando se alcanza este umbral.	30 días	vpxd.certmgmt.certs.cn.hardThreshold
Intervalo de medición de las comprobaciones de validez de certificados de vCenter Server.	5 días	vpxd.certmgmt.certs.cn.pollIntervalDays
Umbral flexible para la caducidad de los certificados. vCenter Server activa un evento cuando se alcanza este umbral.	240 días	vpxd.certmgmt.certs.cn.softThreshold
Modo en que los usuarios de vCenter Server determinan si los certificados existentes deben reemplazarse. Cambie este modo para conservar los certificados durante la actualización. Consulte Certificados y actualizaciones de hosts.	vmca También puede especificar el modo de huella digital o personalizado. Consulte Cambiar el modo de certificado.	modo de vpxd.certmgmt.

Cambiar configuración predeterminada de certificados

Cuando se agrega un host al sistema vCenter Server, vCenter Server envía una solicitud de firma de certificado (CSR) para el host en VMCA. Se puede cambiar parte de la configuración predeterminada en la CSR a través de la configuración avanzada de vCenter Server en vSphere Client.

Consulte Configuración predeterminada de certificados ESXi para obtener una lista de los ajustes predeterminados. Algunos de los valores predeterminados no se pueden cambiar.

Procedimiento

1 En vSphere Client, seleccione el sistema vCenter Server que administra los hosts.

2 Haga clic en **Configurar** y en **Configuración avanzada**.

3 Haga clic en **Editar configuración**.

4 Haga clic en el icono **Filtrar** en la columna Nombre; en el cuadro Filtrar, escriba **`vpxd.certmgmt`** para que se muestren únicamente los parámetros de administración de certificados.

5 Cambie el valor de los parámetros actuales para cumplir con la directiva de la empresa y haga clic en **Guardar**.

   La próxima vez que se agregue un host a vCenter Server, la nueva configuración se utilizará en la CSR que vCenter Server envía a VMCA y en el certificado que se asigna al host.

Pasos siguientes

Los cambios en los metadatos de los certificados solo afectan a los nuevos certificados. Si desea cambiar los certificados de los hosts que ya se administran mediante el sistema vCenter Server, desconecte los hosts y vuelva a conectarlos, o bien renueve los certificados.

Ver la información de caducidad de certificados de varios hosts ESXi

Si utiliza ESXi 6.0 o versiones posteriores, puede ver el estado de los certificados de todos los hosts que administra el sistema vCenter Server. Esta visualización permite determinar si alguno de los certificados está por caducar.

Es posible ver la información del estado de los certificados de los hosts que usan el modo VMCA y los hosts que usan el modo personalizado en vSphere Client. No se puede ver la información del estado de los certificados de los hosts que están en modo de huella digital.

Procedimiento

1. Inicie sesión en vCenter Server mediante vSphere Client.
2. Examine la lista de inventario y seleccione la instancia de vCenter Server.
3. Seleccione **Hosts y clústeres > Hosts**.

   De forma predeterminada, la pantalla Hosts no incluye el estado de los certificados.
4. Haga clic en la flecha hacia abajo en un encabezado de columna para mostrar u ocultar las columnas.
5. Seleccione la casilla **Certificado válido hasta** y desplácese hacia la derecha, si es necesario.

   La información del certificado muestra la fecha de caducidad del certificado.

   Si un host se agrega a vCenter Server o se vuelve a conectar después de una desconexión, vCenter Server renueva el certificado siempre y cuando el estado sea Caducado, En caducidad, Por caducar o Caducidad inminente. El estado es Expiring si el certificado es válido durante menos de ocho meses, Expiring shortly si el certificado es válido durante menos de dos meses y Expiration imminent si el certificado es válido durante menos de un mes.
6. (opcional) Anule la selección de las demás columnas para que le sea más fácil ver lo que le interesa.

Pasos siguientes

Renueve los certificados que estén por caducar. Consulte Renovar o actualizar de certificados de ESXi.

Ver los detalles de certificado para un host único de ESXi

En los hosts ESXi 6.0 y las versiones posteriores en modo VMCA o modo personalizado, se pueden ver los detalles de los certificados desde vSphere Client. La información de los certificados puede resultar útil para las tareas de depuración.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En **Sistema**, haga clic en **Certificado**.

Puede examinar la siguiente información. Esta información está disponible únicamente en la vista de host único.

Campo	Descripción
Asunto	El asunto usado durante la generación del certificado.
Emisor	El emisor del certificado.
Válido desde	La fecha en la que se generó el certificado.
Válido hasta	La fecha en la que caduca el certificado.
Estado	El estado del certificado, que puede ser: **Bueno** Funcionamiento normal. **Por caducar** El certificado caducará pronto. **Por caducar en breve** El certificado caducará en ocho meses o menos (valor predeterminado). **Caducidad inminente** El certificado caducará en dos meses o menos (valor predeterminado). **Caducó** El certificado no es válido porque ya caducó.

Renovar o actualizar de certificados de ESXi

Si VMCA firma certificados en sus hosts ESXi (6.0 y versiones posteriores), puede renovar dichos certificados desde vSphere Client. También puede actualizar todos los certificados del almacén TRUSTED_ROOTS asociado con vCenter Server.

Puede renovar los certificados cuando estos estén por caducar o si desea aprovisionar el host con un certificado nuevo por otros motivos. Si el certificado ya caducó, debe desconectar el host y volverlo a conectar.

De forma predeterminada, vCenter Server renueva los certificados de un host con estado Caducada, En caducidad inmediata o En caducidad cada vez que el host se agrega al inventario o se vuelve a conectar.

Requisitos previos

Compruebe lo siguiente:

- Los hosts ESXi están conectados al sistema vCenter Server.
- La sincronización de hora que se produce entre el sistema vCenter Server y los hosts ESXi es la adecuada.
- La resolución de DNS funciona entre el sistema vCenter Server y los hosts ESXi.
- Los certificados Trusted_Root y MACHINE_SSL_CERT del sistema vCenter Server son válidos y no han caducado. Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2111411.
- Los hosts ESXi no están en modo de mantenimiento.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En **Sistema**, haga clic en **Certificado**.

   Puede ver información detallada sobre el certificado del host seleccionado.

4 Haga clic en **Renovar** o **Actualizar certificados de CA**.

Opción	Descripción
Renew	Recupera un certificado recién firmado desde VMCA para el host.
Actualiza los certificados de CA	Envía todos los certificados del almacén TRUSTED_ROOTS del almacén vCenter Server VECS al host.

5 Haga clic en **Sí** para confirmar.

Cambiar el modo de certificado

Utilice VMCA para aprovisionar los hosts ESXi en su entorno, a menos que la directiva corporativa requiera que use certificados personalizados. En ese caso, para usar certificados personalizados con otra entidad de certificación raíz, puede editar la opción avanzada `vpxd.certmgmt.mode` de vCenter Server. Tras aplicar el cambio, los hosts dejarán de aprovisionarse automáticamente con certificados de VMCA cuando se actualicen los certificados y usted será responsable de administrar los certificados del entorno.

Puede utilizar la configuración avanzada de vCenter Server para cambiar al modo de huella digital o al modo de entidad de certificación personalizada. Utilice el modo de huella digital únicamente como opción de reserva.

Procedimiento

1 En vSphere Client, seleccione el sistema vCenter Server que administra los hosts.

2 Haga clic en **Configurar** y en Configuración, haga clic en **Configuración avanzada**.

3 Haga clic en **Editar configuración**.

4 Haga clic en el icono **Filtrar** en la columna Nombre; en el cuadro Filtrar, escriba **`vpxd.certmgmt`** para que se muestren únicamente los parámetros de administración de certificados.

5 Cambie el valor de `vpxd.certmgmt.mode` a **personalizado** si desea administrar sus propios certificados o a **huella digital** si desea utilizar el modo de huella digital temporalmente. Después, haga clic en **Guardar**.

6 Reinicie el servicio de vCenter Server.

Reemplazo de certificados y claves SSL de ESXi

La directiva de seguridad de su empresa puede requerir que reemplace el certificado SSL predeterminado de ESXi por un certificado firmado por una CA externa en cada host.

De forma predeterminada, los componentes de vSphere utilizan el certificado firmado por VMCA y la clave que se crean durante la instalación. Si elimina el certificado firmado por VMCA de forma accidental, quite el host de su sistema vCenter Server y vuelva a agregarlo. Al agregar el host, vCenter Server solicita un certificado nuevo de VMCA y aprovisiona el host con este certificado.

Reemplace los certificados firmados por VMCA por certificados de una CA de confianza, ya sea una CA comercial o una CA organizativa, si la directiva de su empresa lo requiere.

Los certificados predeterminados están en la misma ubicación que los certificados de vSphere 5.5. Puede reemplazar los certificados predeterminados por certificados de confianza de varias maneras.

Nota También puede utilizar los objetos administrados `vim.CertificateManager` y `vim.host.CertificateManager` en vSphere Web Services SDK. Consulte la documentación de vSphere Web Services SDK.

Después de reemplazar el certificado, debe actualizar el almacén TRUSTED_ROOTS de VECS en el sistema vCenter Server que administra el host, para que vCenter Server y el host ESXi tengan una relación de confianza.

Para obtener instrucciones detalladas sobre el uso de certificados firmados por CA para los hosts ESXi, consulte Flujos de trabajo de cambio de modo de certificado.

Nota Si va a reemplazar certificados SSL en un host ESXi que forma parte de un clúster de vSAN, siga los pasos que se indican en el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/56441.

- Requisitos de las solicitudes de firma de certificados de ESXi

  Si desea utilizar un certificado de empresa o un certificado firmado por entidades de certificación externas, debe enviar una solicitud de firma del certificado (CSR) a la CA.

- Reemplazar el certificado y de la clave predeterminados de ESXi Shell

  Puede reemplazar los certificados firmados por VMCA predeterminados de ESXi en ESXi Shell.

- Reemplazo de la clave y el certificado predeterminados con el comando vifs

  Puede reemplazar los certificados de ESXi firmados por VMCA predeterminados con el comando `vifs`.

- Reemplazar un certificado predeterminado mediante el método PUT de HTTPS

  Puede usar aplicaciones de terceros para cargar certificados y claves. Las aplicaciones que admiten las operaciones del método PUT de HTTPS funcionan con la interfaz de HTTPS incluida en ESXi.

- Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados)

  Si configura los hosts ESXi para usar certificados personalizados, debe actualizar el almacén `TRUSTED_ROOTS` en el sistema vCenter Server que administra los hosts.

Requisitos de las solicitudes de firma de certificados de ESXi

Si desea utilizar un certificado de empresa o un certificado firmado por entidades de certificación externas, debe enviar una solicitud de firma del certificado (CSR) a la CA.

Utilice una CSR con estas características:

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)
- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
- x509 versión 3
- Para los certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos.
- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Formato CRT
- Contiene los siguientes usos de claves: firma digital, no repudio, cifrado de clave
- Hora de inicio de un día anterior a la hora actual.
- CN (y SubjectAltName) establecidos con el nombre de host (o dirección IP) que el host ESXi tiene en el inventario de vCenter Server.

Para obtener información sobre cómo generar el servicio CSR, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2113926.

Reemplazar el certificado y de la clave predeterminados de ESXi Shell

Puede reemplazar los certificados firmados por VMCA predeterminados de ESXi en ESXi Shell.

Requisitos previos

- Si desea usar certificados firmados por una entidad de certificación (CA) externa, genere la solicitud de certificación, envíela a la entidad de certificación y almacene los certificados en cada host ESXi.
- De ser necesario, habilite ESXi Shell o el tráfico SSH desde vSphere Client.
- Todas las transferencias de archivos y demás comunicaciones se realizan en una sesión de HTTPS segura. El usuario que se usa para autenticar la sesión debe tener el privilegio **Host.Configuración.Configuración avanzada** en el host.

Procedimiento

1 Inicie sesión en ESXi Shell, ya sea directamente desde la DCUI o desde un cliente de SSH, como un usuario con privilegios de administrador.

2 En el directorio `/etc/vmware/ssl`, cambie el nombre de los certificados existentes con los siguientes comandos.

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

3 Copie los certificados que desea utilizar en `/etc/vmware/ssl`.

4 Cambie el nombre del certificado nuevo y de la clave por `rui.crt` y `rui.key`.

5 Después de instalar el certificado nuevo, reinicie el host.

Como alternativa, puede colocar el host en modo de mantenimiento, instalar el certificado nuevo, utilizar la interfaz de usuario de la consola directa (DCUI) para reiniciar los agentes de administración y, a continuación, establecer el host para que salga del modo de mantenimiento.

Pasos siguientes

Actualice el almacén vCenter Server TRUSTED_ROOTS. Consulte Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados).

Reemplazo de la clave y el certificado predeterminados con el comando vifs

Puede reemplazar los certificados de ESXi firmados por VMCA predeterminados con el comando `vifs`.

Ejecute `vifs` como comando de vCLI. Consulte la *Referencia de la interfaz de línea de comandos de vSphere*.

Requisitos previos

- Si desea usar certificados firmados por una entidad de certificación (CA) externa, genere la solicitud de certificación, envíela a la entidad de certificación y almacene los certificados en cada host ESXi.

- De ser necesario, habilite ESXi Shell o el tráfico SSH desde vSphere Client.
- Todas las transferencias de archivos y demás comunicaciones se realizan en una sesión de HTTPS segura. El usuario que se usa para autenticar la sesión debe tener el privilegio **Host.Configuración.Configuración avanzada** en el host.

Procedimiento

1 Realice una copia de seguridad de los certificados actuales.

2 Genere la solicitud de certificación con las instrucciones de la entidad de certificación.

   Consulte Requisitos de las solicitudes de firma de certificados de ESXi.

3 Cuando tenga el certificado, use el comando `vifs` para cargar el certificado en la ubicación adecuada del host a través de una conexión SSH.

   ```
   vifs --server hostname --username username --put rui.crt /host/ssl_cert
   vifs --server hostname --username username --put rui.key /host/ssl_key
   ```

4 Reinicie el host.

   Como alternativa, puede colocar el host en modo de mantenimiento, instalar el certificado nuevo, utilizar la interfaz de usuario de la consola directa (DCUI) para reiniciar los agentes de administración y, a continuación, establecer el host para que salga del modo de mantenimiento.

Pasos siguientes

Actualice el almacén vCenter Server TRUSTED_ROOTS. Consulte Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados).

Reemplazar un certificado predeterminado mediante el método PUT de HTTPS

Puede usar aplicaciones de terceros para cargar certificados y claves. Las aplicaciones que admiten las operaciones del método PUT de HTTPS funcionan con la interfaz de HTTPS incluida en ESXi.

Requisitos previos

- Si desea usar certificados firmados por una entidad de certificación (CA) externa, genere la solicitud de certificación, envíela a la entidad de certificación y almacene los certificados en cada host ESXi.
- De ser necesario, habilite ESXi Shell o el tráfico SSH desde vSphere Client.
- Todas las transferencias de archivos y demás comunicaciones se realizan en una sesión de HTTPS segura. El usuario que se usa para autenticar la sesión debe tener el privilegio **Host.Configuración.Configuración avanzada** en el host.

Procedimiento

1 Realice una copia de seguridad de los certificados actuales.

2 En la aplicación de carga, procese cada archivo de la siguiente manera:

   a Abra el archivo.

   b Publique el archivo en una de estas ubicaciones.

Opción	Descripción
Certificados	`https://hostname/host/ssl_cert`
Claves	`https://hostname/host/ssl_key`

   Las ubicaciones `/host/ssl_cert` y `host/ssl_key` conducen a los archivos de certificado en `/etc/vmware/ssl`.

3 Reinicie el host.

   Como alternativa, puede colocar el host en modo de mantenimiento, instalar el certificado nuevo, utilizar la interfaz de usuario de la consola directa (DCUI) para reiniciar los agentes de administración y, a continuación, establecer el host para que salga del modo de mantenimiento.

Pasos siguientes

Actualice el almacén vCenter Server TRUSTED_ROOTS. Consulte Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados).

Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados)

Si configura los hosts ESXi para usar certificados personalizados, debe actualizar el almacén `TRUSTED_ROOTS` en el sistema vCenter Server que administra los hosts.

Requisitos previos

Reemplace los certificados de cada host por los certificados personalizados.

Nota Este paso no es necesario si el sistema vCenter Server también se ejecuta con certificados personalizados emitidos por la misma entidad de certificación que los instalados en los hosts ESXi.

Procedimiento

1 Inicie sesión en el sistema vCenter Server que administra los hosts ESXi.

   Inicie sesión en el sistema Windows en el que instaló el software, o en el shell de vCenter Server Appliance.

2 Para agregar los nuevos certificados al almacén TRUSTED_ROOTS, ejecute dir-cli, por ejemplo:

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish <path_to_RootCA>
```

Opción	Descripción
Linux	//usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish <path_to_RootCA>
Windows	C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli trustedcert publish <path_to_RootCA>

3 Cuando se le solicite, proporcione las credenciales de administrador de Single Sign-On.

4 Si los certificados personalizados son emitidos por una entidad de certificación intermedia, también debe agregar esta entidad al almacén TRUSTED_ROOTS en vCenter Server, por ejemplo:

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish <path_to_intermediateCA>
```

Pasos siguientes

Establezca el modo de certificación en Personalizado. Si el modo de certificación es VCMA (valor predeterminado) y ejecuta una actualización de certificados, los certificados personalizados se reemplazan por los certificados firmados por VMCA. Consulte Cambiar el modo de certificado.

Usar certificados personalizados con Auto Deploy

De manera predeterminada, el servidor Auto Deploy aprovisiona cada host con certificados firmados por VMCA. Es posible configurar el servidor Auto Deploy para que aprovisione todos los hosts con certificados personalizados que no estén firmados por VMCA. En ese caso, el servidor Auto Deploy se transforma en una entidad de certificación subordinada a la entidad de certificación externa.

Requisitos previos

- Solicite a la CA un certificado. El certificado debe cumplir con estos requisitos.
  - Tamaño de clave: 2.048 bits o más (formato codificado PEM)
  - Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
  - x509 versión 3
  - Para los certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos.
  - SubjectAltName debe contener DNS Name=<machine_FQDN>.

- Formato CRT
- Contiene los siguientes usos de claves: firma digital, no repudio, cifrado de clave
- Hora de inicio de un día anterior a la hora actual.
- CN (y SubjectAltName) establecidos con el nombre de host (o dirección IP) que el host ESXi tiene en el inventario de vCenter Server.

- Asigne un nombre para el certificado y los archivos de claves `rbd-ca.crt` y `rbd-ca.key`.

Procedimiento

1 Realice una copia de seguridad de los certificados de ESXi predeterminados.

Los certificados están en el directorio `/etc/vmware-rbd/ssl/`.

2 Detenga el servicio de vSphere Authentication Proxy.

Herramienta	Pasos
Interfaz de administración de vCenter Server Appliance (VAMI)	a En un explorador web, vaya a la interfaz de administración de vCenter Server Appliance, https://*dirección-IP-o-FQDN-de-dispositivo*:5480. b Inicie sesión como raíz. La contraseña raíz predeterminada es la que estableció al implementar vCenter Server Appliance. c Haga clic en **Servicios** y en el servicio **VMware vSphere Authentication Proxy**. d Haga clic en **Detener**.
vSphere Web Client	a Seleccione **Administración** y haga clic en **Configuración del sistema** en **Implementación**. b Haga clic en **Servicios** y en el servicio **VMware vSphere Authentication Proxy**. c Haga clic en el icono rojo **Detener el servicio**.
CLI	`service-control --stop vmcam`

3 En el sistema donde se ejecuta el servicio de Auto Deploy, reemplace `rbd-ca.crt` y `rbd-ca.key` en `/etc/vmware-rbd/ssl/` por el certificado personalizado y los archivos de claves.

4 En el sistema donde se ejecuta el servicio de Auto Deploy, ejecute los siguientes comandos a fin de actualizar el almacén TRUSTED_ROOTS en VECS para utilizar los nuevos certificados.

Opción	Descripción

Windows	`cd "C:\Program Files\VMware\vCenter Server\vmafdd\"`
	`.\dir-cli.exe trustedcert publish --cert C:\ProgramData\VMware\vCenterServer\data\autodeploy\ssl\rbd-ca.crt`
	`.\vecs-cli force-refresh`

Linux	`/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert /etc/vmware-rbd/ssl/rbd-ca.crt` `/usr/lib/vmware-vmafd/bin/vecs-cli force-refresh`

5 Cree un archivo `castore.pem` que incluya el contenido del almacén TRUSTED_ROOTS y coloque el archivo en el directorio `/etc/vmware-rbd/ssl/`.

   En el modo personalizado, usted es responsable de mantener este archivo.

6 Cambie el modo de certificación de ESXi del sistema de vCenter Server a **`custom`**.

   Consulte Cambiar el modo de certificado.

7 Reinicie el servicio de vCenter Server e inicie el servicio de Auto Deploy.

Resultados

La próxima vez que aprovisione un host que esté configurado para usar Auto Deploy, el servidor Auto Deploy generará un certificado. El servidor Auto Deploy utiliza el certificado de raíz que acaba de agregar al almacén TRUSTED_ROOTS.

Nota Si tiene problemas con Auto Deploy después de reemplazar el certificado, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2000988.

Restaurar archivos de certificados y claves de ESXi

Al reemplazar un certificado en un host ESXi mediante vSphere Web Services SDK, el certificado y la clave anteriores se anexan a un archivo `.bak`. Para restaurar certificados anteriores, mueva la información del archivo `.bak` al archivo actual de certificados y claves.

El certificado y la clave del host se encuentran en `/etc/vmware/ssl/rui.crt` y `/etc/vmware/ssl/rui.key`. Al reemplazar el certificado y la clave de un host mediante el objeto administrado `vim.CertificateManager` de vSphere Web Services SDK, la clave y el certificado anteriores se anexan al archivo `/etc/vmware/ssl/rui.bak`.

Nota Si reemplaza el certificado con HTTP PUT, `vifs` o desde ESXi Shell, los certificados existentes no se anexan al archivo `.bak`.

Procedimiento

1. En el host ESXi, busque el archivo `/etc/vmware/ssl/rui.bak`.

   El archivo tiene el siguiente formato.

   ```
   #
   # Host private key and certificate backup from 2014-06-20 08:02:49.961
   #

   -----BEGIN PRIVATE KEY-----
   previous key
   -----END PRIVATE KEY-----

   -----BEGIN CERTIFICATE-----
   previous cert
   -----END CERTIFICATE-----
   ```

2. Copie el texto que empieza con `-----BEGIN PRIVATE KEY-----` y termina con `-----END PRIVATE KEY-----` en el archivo `/etc/vmware/ssl/rui.key`.

   Incluya `-----BEGIN PRIVATE KEY-----` y `-----END PRIVATE KEY-----`.

3. Copie el texto que está entre `-----BEGIN CERTIFICATE-----` y `-----END CERTIFICATE-----` en el archivo `/etc/vmware/ssl/rui.crt`.

   Incluya `-----BEGIN CERTIFICATE-----` y `-----END CERTIFICATE-----`.

4. Reinicie el host de ESXi.

   Como alternativa, puede colocar el host en modo de mantenimiento y utilizar la interfaz de usuario de la consola directa (DCUI) para reiniciar los agentes de administración y, a continuación, establecer el host para que salga del modo de mantenimiento.

Personalizar hosts con el perfil de seguridad

Puede personalizar muchos de los ajustes de seguridad fundamentales para el host mediante los paneles Perfil de seguridad, Servicios y Firewall, disponibles en vSphere Client. El perfil de seguridad es especialmente útil para la administración de un host único. Si debe administrar varios hosts, considere utilizar una de las CLI o los SDK y automatizar las tareas de personalización.

Configurar firewalls de ESXi

ESXi incluye un firewall que está habilitado de forma predeterminada.

En el momento de realizar la instalación, el firewall de ESXi se configura para bloquear el tráfico entrante y saliente, excepto el tráfico de los servicios que están habilitados en el perfil de seguridad del host.

Al abrir puertos en el firewall, tenga en cuenta que el acceso no restringido a los servicios que se ejecutan en un host ESXi pueden exponer un host a ataques externos y acceso no autorizado. Para reducir el riesgo, configure el firewall de ESXi para que permita el acceso solo desde redes autorizadas.

Nota El firewall también permite pings del protocolo Control Message Protocol (ICMP) y la comunicación con los clientes DHCP y DNS (solo UDP).

Es posible administrar puertos de firewall de ESXi de la siguiente manera:

- Utilice las opciones **Configurar > Firewall** para cada host en vSphere Client. Consulte Administrar la configuración del firewall de ESXi.
- Utilice los comandos ESXCLI en la línea de comandos o en los scripts. Consulte Comandos de firewall ESXCLI de ESXi.
- Utilice un VIB si el puerto que desea abrir no está incluido en el perfil de seguridad.

  Puede crear VIB personalizados con la herramienta VIB Author disponible en VMware Labs. Para instalar el VIB personalizado, se debe cambiar el nivel de aceptación del host ESXi a CommunitySupported.

  Nota Si se contacta con el soporte técnico de VMware para investigar un problema en un host ESXi con un VIB CommunitySupported instalado, el soporte de VMware puede solicitarle que desinstale este VIB. Dicha solicitud es un paso de solución de problemas para determinar si ese VIB está relacionado con el problema que se investiga.

Conceptos del firewall de ESXi (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_m5fueehb/uiConfId/49694343/)

El comportamiento del conjunto de reglas del cliente NFS (`nfsClient`) es diferente a otros conjuntos de reglas. Cuando el conjunto de reglas del cliente NFS está habilitado, todos los puertos TCP salientes están abiertos para los hosts de destino que se incluyen en la lista de direcciones IP permitidas. Consulte Comportamiento de firewall del cliente NFS para obtener más información.

Administrar la configuración del firewall de ESXi

Puede configurar conexiones entrantes o salientes en el firewall para un servicio o un agente de administración desde vSphere Client, vSphere Web Client o en la línea de comandos.

Nota Si hay distintos servicios con reglas de puerto superpuestas, al habilitar un servicio, es posible que se habiliten otros servicios de forma implícita. Para evitar este problema, se pueden especificar qué direcciones IP tienen permiso para acceder a cada servicio en el host.

Procedimiento

1 Desplácese hasta el host en el inventario.

2 Desplácese hasta la sección Firewall.

Opción	Descripción
vSphere Client	a Haga clic en **Configurar**. b En Sistema, haga clic en **Firewall**.
vSphere Web Client	a Haga clic en **Configurar**. b En Sistema, haga clic en **Perfil de seguridad**. c Si es necesario, desplácese hasta la sección Firewall.

La pantalla muestra una lista de conexiones activas entrantes y salientes con los correspondientes puertos de firewall.

3 En la sección Firewall, haga clic en **Editar**.

La pantalla muestra los conjuntos de reglas de firewall, que incluyen el nombre de la regla y la información asociada.

4 Seleccione los conjuntos de reglas para habilitarlos o desactive la casilla para deshabilitarlos.

5 En algunos servicios, también es posible administrar los detalles de servicio.

Opción	Descripción
vSphere Client	Puede administrar los detalles del servicio desde **Configurar > Servicios** en Sistema.
vSphere Web Client	En la sección Detalles de servicio, puede realizar lo siguiente: ■ Utilice los botones **Iniciar**, **Detener** o **Reiniciar** para cambiar el estado de un servicio temporalmente. ■ Cambie la directiva de inicio para que el servicio se inicie con el host o con la utilización de puertos.

Para obtener más información sobre la forma de iniciar, detener y reiniciar los servicios, consulte Habilitar o deshabilitar un servicio.

6 Para algunos servicios, se pueden especificar explícitamente las direcciones IP para las que se permiten conexiones.

Consulte Agregar direcciones IP permitidas para un host ESXi.

7 Haga clic en **Aceptar**.

Agregar direcciones IP permitidas para un host ESXi

De forma predeterminada, el firewall de cada servicio permite el acceso a todas las direcciones IP. Para restringir el tráfico, cambie cada servicio para permitir el tráfico solo desde la subred de administración. También puede anular la selección de algunos servicios si el entorno no los usa.

Puede usar vSphere Client, vSphere Web Client, vCLI o PowerCLI para actualizar la lista de direcciones IP permitidas para un servicio. De forma predeterminada, todas las direcciones IP están permitidas para un servicio. Esta tarea describe la forma de utilizar vSphere Client o vSphere Web Client. Consulte el tema sobre cómo administrar el firewall en *Conceptos y ejemplos de la interfaz de línea de comandos de vSphere* en https://code.vmware.com/ para obtener instrucciones sobre cómo utilizar la vCLI.

Agregar direcciones IP permitidas al firewall de ESXi (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_2lu2gk6g/uiConfId/49694343/)

Procedimiento

1 Desplácese hasta el host en el inventario.

2 Desplácese hasta la sección Firewall.

Opción	Descripción
vSphere Client	a Haga clic en **Configurar**. b En Sistema, haga clic en **Firewall**.
vSphere Web Client	a Haga clic en **Configurar**. b En Sistema, haga clic en **Perfil de seguridad**. c Si es necesario, desplácese hasta la sección Firewall.

3 En la sección Firewall, haga clic en **Editar** y seleccione un servicio de la lista.

4 En la sección Direcciones IP permitidas, desactive la casilla **Permitir conexiones desde cualquier dirección IP** e introduzca las direcciones IP de las redes que tienen permiso para conectarse al host.

   Separe las direcciones IP con comas. Puede utilizar los siguientes formatos de dirección:

   - 192.168.0.0/24
   - 192.168.1.2, 2001::1/64
   - fd3e:29a6:0a81:e478::/64

5 Haga clic en **Aceptar**.

Puertos de firewall entrantes y salientes para hosts de ESXi

vSphere Client, vSphere Web Client y VMware Host Client permiten abrir y cerrar puertos de firewall para cada servicio o admitir el tráfico procedente de las direcciones IP seleccionadas.

ESXi incluye un firewall que está habilitado de forma predeterminada. En el momento de realizar la instalación, el firewall de ESXi se configura para bloquear el tráfico entrante y saliente, excepto el tráfico de los servicios que están habilitados en el perfil de seguridad del host. Para obtener la lista de los puertos y protocolos compatibles en el firewall de ESXi, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/.

La herramienta VMware Ports and Protocols muestra la información sobre los puertos de los servicios que se instalan de forma predeterminada. Si instala otros VIB en el host, es posible que estén disponibles otros puertos de firewall y servicios adicionales. La información es principalmente para los servicios que están visibles en vSphere Client y vSphere Web Client, pero la herramienta VMware Ports and Protocols también incluye otros puertos.

Comportamiento de firewall del cliente NFS

El conjunto de reglas de firewall del cliente NFS se comporta de forma diferente a otros conjuntos de reglas de firewall de ESXi. ESXi configura los parámetros del cliente NFS cuando se monta o desmonta una almacén de datos de NFS. El comportamiento varía según la versión de NFS.

Cuando se agrega, monta o desmonta un almacén de datos de NFS, el comportamiento que se obtiene varía según la versión de NFS.

Comportamiento de firewall de NFS v3

Cuando se agrega o monta un almacén de datos de NFS v3, ESXi comprueba el estado del conjunto de reglas de firewall del cliente NFS (`nfsClient`).

- Si el conjunto de reglas `nfsClient` está deshabilitado, ESXi habilita el conjunto de reglas y deshabilita la directiva Permitir todas las direcciones IP estableciendo la marca `allowedAll` en `FALSE`. La dirección IP del servidor NFS se agrega a la lista de direcciones IP salientes permitidas.
- Si el conjunto de reglas `nfsClient` está habilitado, el estado del conjunto de reglas y la directiva de direcciones IP permitidas no se cambian. La dirección IP del servidor NFS se agrega a la lista de direcciones IP salientes permitidas.

Nota Si habilita manualmente el conjunto de reglas `nfsClient` o configura manualmente la directiva Permitir todas las direcciones IP, ya sea antes o después de agregar un almacén de datos de NFS v3 al sistema, la configuración se anula cuando se desmonta el último almacén de datos de NFS v3. El conjunto de reglas `nfsClient` se deshabilita cuando se desmontan todos los almacenes de datos de NFS v3.

Cuando se quita o se desmonta un almacén de datos de NFS v3, ESXi realiza una de las siguientes acciones.

- Si ninguno de los almacenes de datos de NFS v3 restantes se monta desde el servidor del almacén de datos que se desmonta, ESXi quita la dirección IP del servidor de la lista de direcciones IP salientes.
- Si ninguno de los almacenes de datos de NFS v3 permanece después de la operación de desmontaje, ESXi deshabilita el conjunto de reglas de firewall de `nfsClient`.

Comportamiento de firewall de NFS v4.1

Cuando se monta el primer almacén de datos NFS v4.1, ESXi habilita el conjunto de reglas `nfs41client` y establece su marca `allowedAll` en TRUE. Esta acción abre el puerto 2049 para todas las direcciones IP. Cuando se desmonta el almacén de datos NFS v4.1, el estado del firewall no se ve afectado. De esta forma, el primer montaje de NFS v4.1 abre el puerto 2049, y ese puerto permanece habilitado a menos que se cierre explícitamente.

Comandos de firewall ESXCLI de ESXi

Si el entorno incluye varios hosts ESXi, se recomienda automatizar la configuración del firewall mediante los comandos ESXCLI o vSphere Web Services SDK.

Referencia de comandos de firewall

Se pueden utilizar los comandos de ESXi Shell o vSphere CLI en la línea de comandos para configurar ESXi a fin de automatizar la configuración del firewall. Consulte *Introducción a ESXCLI* para ver una introducción y *Ejemplos y conceptos de vSphere Command-Line Interface* para ver ejemplos de uso de ESXCLI para administrar firewalls y reglas de firewall. Consulte el artículo 2008226 de la base de conocimientos de VMware para obtener más información sobre cómo crear reglas de firewall personalizadas.

Tabla 3-4. Comandos de firewall

Comando	Descripción
`esxcli network firewall get`	Devuelve el estado habilitado o deshabilitado del firewall y enumera las acciones predeterminadas.
`esxcli network firewall set --default-action`	Se establece en true para definir que la acción predeterminada sea pasar. Se establece en false para definir que la acción predeterminada sea anular.
`esxcli network firewall set --enabled`	Habilita o deshabilita el firewall de ESXi.
`esxcli network firewall load`	Carga los archivos de configuración del conjunto de módulos y reglas del firewall.
`esxcli network firewall refresh`	Actualiza la configuración del firewall mediante la lectura de los archivos del conjunto de reglas si se carga el módulo de firewall.
`esxcli network firewall unload`	Destruye los filtros y descarga el módulo de firewall.
`esxcli network firewall ruleset list`	Enumera la información de los conjuntos de reglas.
`esxcli network firewall ruleset set --allowed-all`	Se establece en true para permitir un acceso total a todas las direcciones IP, o en false para utilizar una lista de direcciones IP permitidas.
`esxcli network firewall ruleset set --enabled --ruleset-id=<string>`	Se establece en true para habilitar el conjunto de reglas especificado. Se establece en false para deshabilitar el conjunto de reglas especificado.
`esxcli network firewall ruleset allowedip list`	Enumera las direcciones IP permitidas del conjunto de reglas especificado.

Tabla 3-4. Comandos de firewall (continuación)

Comando	Descripción
`esxcli network firewall ruleset allowedip add`	Permite acceder al conjunto de reglas desde la dirección IP o el intervalo de direcciones IP especificado.
`esxcli network firewall ruleset allowedip remove`	Quita el acceso al conjunto de reglas desde la dirección IP o el intervalo de direcciones IP especificados.
`esxcli network firewall ruleset rule list`	Enumera las reglas de cada conjunto de reglas del firewall.

Ejemplos de comandos de firewall

Los siguientes ejemplos se han extraído de la publicación de un blog en virtuallyGhetto.

1 Compruebe que hay un conjunto de reglas nuevo llamado virtuallyGhetto.

```
esxcli network firewall ruleset rule list | grep virtuallyGhetto
```

2 Especifique los rangos de IP o la dirección IP específica para acceder a un servicio particular. En el siguiente ejemplo se deshabilita la opción `allow all` y se especifica un intervalo determinado para el servicio virtuallyGhetto.

```
esxcli network firewall ruleset set --allowed-all false --ruleset-id=virtuallyGhetto
esxcli network firewall ruleset allowedip add --ip-address=172.30.0.0/24 --ruleset-
id=virtuallyGhetto
```

Personalizar los servicios de ESXi desde el perfil de seguridad

Un host ESXi incluye varios servicios que se ejecutan de manera predeterminada. Es posible deshabilitar servicios desde el perfil de seguridad o habilitar servicios si la directiva de la empresa lo permite.

Habilitar o deshabilitar un servicio es un ejemplo que muestra cómo habilitar un servicio.

Nota La habilitación de servicios afecta la seguridad del host. No habilite un servicio a menos que sea estrictamente necesario.

Los servicios disponibles dependen de los VIB que están instalados en el host ESXi. No puede agregar servicios sin instalar un VIB. Algunos productos de VMware, por ejemplo vSphere HA, instalan los VIB en los hosts para que los servicios y sus correspondientes puertos de firewall estén disponibles.

En una instalación predeterminada, puede modificar el estado de los siguientes servicios desde vSphere Client.

Tabla 3-5. Servicios de ESXi en el perfil de seguridad

Servicio	Predeterminado	Descripción
Interfaz de usuario de consola directa	En ejecución	El servicio de la interfaz de usuario de la consola directa (DCUI) permite interactuar con un host ESXi desde el host de la consola local mediante menús basados en texto.
ESXi Shell	Detenido	ESXi Shell está disponible desde la DCUI e incluye un conjunto de comandos totalmente compatibles, así como un conjunto de comandos para solucionar problemas y corregir errores. Debe habilitar el acceso a ESXi Shell desde la consola directa de cada sistema. Puede habilitar el acceso a ESXi Shell local o el acceso a ESXi Shell mediante SSH.
SSH	Detenido	El servicio del cliente SSH del host que permite realizar conexiones remotas mediante Secure Shell.
Daemon para la formación de equipos basada en cargas	En ejecución	Formación de equipos basada en cargas.
Servicio de Active Directory	Detenido	Este servicio se inicia al configurar ESXi para Active Directory.
Daemon de NTP	Detenido	Daemon del protocolo Network Time Protocol.
Daemon de tarjeta inteligente PC/SC	Detenido	Este servicio se inicia cuando se habilita el host para la autenticación de tarjeta inteligente. Consulte Configurar la autenticación de tarjeta inteligente de ESXi.
Servidor CIM	En ejecución	Servicio que las aplicaciones del modelo de información común pueden utilizar (CIM).
Servidor SNMP	Detenido	Daemon del SNMP. Consulte *Supervisión y rendimiento de vSphere* para obtener información sobre cómo configurar el SNMP v1, v2 y v3.
Servidor de Syslog	Detenido	Daemon de Syslog. Puede habilitar Syslog desde la configuración avanzada del sistema en vSphere Client. Consulte *Instalar y configurar vCenter Server*.
VMware vCenter Agent	En ejecución	Agente de vCenter Server. Permite que vCenter Server se conecte a un host ESXi. Específicamente, vpxa es el canal de comunicación con el daemon del host que, a su vez, se comunica con el kernel de ESXi.
Servidor X.Org	Detenido	Servidor X.Org. Esta característica opcional es de uso interno para los gráficos 3D de las máquinas virtuales.

Habilitar o deshabilitar un servicio

Puede habilitar o deshabilitar servicios desde vSphere Client o vSphere Web Client.

Después de la instalación, algunos servicios se ejecutan de manera predeterminada, pero otros se interrumpen. En ocasiones, es necesario realizar otro paso de configuración para que el servicio se vuelva disponible en la interfaz de usuario. Por ejemplo, el servicio NTP es una forma de obtener información de tiempo precisa, pero este servicio solamente funciona cuando se abren los puertos requeridos en el firewall.

Requisitos previos

Conéctese a vCenter Server con vSphere Client o vSphere Web Client.

Procedimiento

1 Desplácese hasta un host en el inventario.

2 Desplácese hasta la sección de servicios.

Opción	Descripción
vSphere Client	a Haga clic en **Configurar**. b En Sistema, haga clic en **Servicios**.
vSphere Web Client	a Haga clic en **Configurar**. b En Sistema, haga clic en **Perfil de seguridad**.

3 Administre los servicios.

Opción	Descripción
vSphere Client	a Seleccione el servicio que desee cambiar. b Seleccione **Reiniciar**, **Iniciar** o **Detener** para hacer un cambio por única vez en el estado del host. c Para cambiar el estado del host en todos los reinicios, haga clic en **Editar directiva de inicio** y seleccione una directiva.
vSphere Web Client	a Haga clic en **Editar**. b Desplácese hasta el servicio que desea cambiar. c En el panel Detalles de servicio, seleccione **Iniciar**, **Detener** o **Reiniciar** para realizar un cambio por única vez en el estado del host. d Para cambiar el estado del host en todos los reinicios, seleccione una directiva del menú **Directiva de inicio**.

- **Iniciar y detener con host**: el servicio se inicia poco después de que se enciende el host, y se cierra poco después de que se apaga el host. Al igual que **Iniciar y detener con uso de puerto**, esta opción implica que el servicio intenta regularmente completar sus tareas, como ponerse en contacto con el servidor NTP especificado. Si el puerto se cerró, pero luego se abre, el cliente empieza a completar las tareas poco tiempo después.
- **Iniciar y detener manualmente**: el host conserva la configuración del servicio determinada por el usuario, más allá de que los puertos estén abiertos o cerrados. Cuando un usuario

inicia el servicio NTP, el servicio sigue en ejecución si se enciende el host. Si el servicio se inicia y el host está apagado, el servicio se detiene como parte del proceso de apagado; pero en cuanto el host se enciende, el servicio vuelve a iniciarse, y así se conserva el estado determinado por el usuario.

- **Iniciar y detener con uso de puerto**: el ajuste predeterminado para estos servicios. Si existe algún puerto abierto, el cliente intenta comunicarse con los recursos de red del servicio. Si existen algunos puertos abiertos, pero el puerto de un servicio específico está cerrado, se produce un error en el intento. Si el puerto saliente correspondiente está abierto, el servicio comienza a completar el inicio.

Nota Esta configuración se aplica únicamente a la configuración de servicio establecida mediante la interfaz de usuario o a las aplicaciones creadas en vSphere Web Services SDK. Toda configuración establecida por otros medios, como desde ESXi Shell o mediante archivos de configuración, no se ve afectada por esta configuración.

4 Haga clic en **Aceptar**.

Modo de bloqueo

Para mejorar la seguridad de los hosts ESXi, puede ponerlos en modo de bloqueo. En el modo de bloqueo, las operaciones deben realizarse mediante vCenter Server de forma predeterminada.

A partir de vSphere 6.0, puede seleccionar el modo de bloqueo normal o el modo de bloqueo estricto, que ofrecen diferentes grados de bloqueo. vSphere 6.0 también incluye la lista de usuarios con excepción. Los usuarios con excepción no pierden sus privilegios cuando el host entra en el modo de bloqueo. Utilice la lista de usuarios con excepción para agregar cuentas de soluciones de terceros y aplicaciones externas que deben tener acceso directo al host cuando este último está en modo de bloqueo. Consulte Especificar usuarios con excepción para el modo de bloqueo.

Modo de bloqueo en vSphere 6 (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_zg4ylgu0/uiConfId/49694343/)

Comportamiento del modo de bloqueo

En el modo de bloqueo, algunos dispositivos se deshabilitan y algunos servicios quedan accesibles solo para ciertos usuarios.

Servicios de modo de bloqueo para diferentes usuarios

Cuando el host está en ejecución, los servicios disponibles dependen de si el modo de bloqueo está habilitado y del tipo de modo de bloqueo.

- En los modos de bloqueo estricto y normal, los usuarios con privilegios pueden acceder al host mediante vCenter Server, ya sea desde vSphere Client o vSphere Web Client, o mediante el uso de vSphere Web Services SDK.

- El comportamiento de la interfaz de la consola directa no es igual en el modo de bloqueo estricto que en el modo de bloqueo normal.
  - En el modo de bloqueo estricto, el servicio de interfaz de usuario de la consola directa (DCUI) está deshabilitado.
  - En el modo de bloqueo normal, las cuentas de la lista de usuarios con excepción pueden acceder a la DCUI si poseen privilegios de administrador. Además, todos los usuarios que se especifican en la opción avanzada del sistema `DCUI.Access` pueden acceder a la DCUI.
- Si ESXi Shell o SSH están habilitados y el host se encuentra en el modo de bloqueo, las cuentas de la lista de usuarios con excepción que tienen privilegios de administrador pueden usar estos servicios. Para los demás usuarios, el acceso a ESXi Shell o SSH queda deshabilitado. A partir de vSphere 6.0, se cierran las sesiones de ESXi o SSH de los usuarios que no tienen privilegios de administrador.

Todas las operaciones de acceso se registran para ambos modos de bloqueo, estricto y normal.

Tabla 3-6. Comportamiento del modo de bloqueo

Servicio	Modo normal	Modo de bloqueo normal	Modo de bloqueo estricto
vSphere Web Services API	Todos los usuarios, según los permisos	vCenter (vpxuser) Usuarios con excepción, según los permisos vCloud Director (vslauser, si está disponible)	vCenter (vpxuser) Usuarios con excepción, según los permisos vCloud Director (vslauser, si está disponible)
Proveedores de CIM	Usuarios con privilegios de administrador en el host	vCenter (vpxuser) Usuarios con excepción, según los permisos. vCloud Director (vslauser, si está disponible)	vCenter (vpxuser) Usuarios con excepción, según los permisos. vCloud Director (vslauser, si está disponible)
UI de consola directa (DCUI)	Usuarios con privilegios de administrador en el host y usuarios que se encuentran en la opción avanzada `DCUI.Access`	Usuarios definidos en la opción avanzada `DCUI.Access` Usuarios con excepción con privilegios de administrador en el host	El servicio de DCUI se detiene.
ESXi Shell (si está habilitado)	Usuarios con privilegios de administrador en el host	Usuarios definidos en la opción avanzada `DCUI.Access` Usuarios con excepción con privilegios de administrador en el host	Usuarios definidos en la opción avanzada `DCUI.Access` Usuarios con excepción con privilegios de administrador en el host
SSH (si está habilitado)	Usuarios con privilegios de administrador en el host	Usuarios definidos en la opción avanzada `DCUI.Access` Usuarios con excepción con privilegios de administrador en el host	Usuarios definidos en la opción avanzada `DCUI.Access` Usuarios con excepción con privilegios de administrador en el host

Usuarios con sesión iniciada en ESXi Shell cuando el modo de bloqueo está habilitado

Los usuarios pueden iniciar sesión en el ESXi Shell o acceder al host a través de SSH antes de habilitar el modo de bloqueo. En ese caso, la sesión de los usuarios que estén en la lista de usuarios con excepción y que tengan privilegios de administrador en el host permanecerá activa. A partir de vSphere 6.0, se cierra la sesión para los demás usuarios. La finalización se aplica tanto al modo de bloqueo normal como al estricto.

Habilitar modo de bloqueo

Habilite el modo de bloqueo para que se requiera que todos los cambios de configuración pasen por vCenter Server. vSphere 6.0 y versiones posteriores admiten el modo de bloqueo normal y el modo de bloqueo estricto.

Si prefiere no permitir todo acceso directo a un host por completo, puede seleccionar el modo de bloqueo estricto. El modo de bloqueo estricto permite el acceso a un host si vCenter Server no está disponible y SSH y ESXi Shell están deshabilitados. Consulte Comportamiento del modo de bloqueo.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Perfil de seguridad**.

4 En el panel Modo de bloqueo, haga clic en **Editar**.

5 Haga clic en **Modo de bloqueo** y seleccione una de las opciones del modo de bloqueo.

Opción	Descripción
Normal	Se puede acceder al host desde vCenter Server. Solo los usuarios que están en la lista de usuarios con excepción y tienen privilegios de administrador pueden iniciar sesión en la interfaz de usuario de la consola directa. Si SSH o ESXi Shell están habilitados, es posible que se pueda tener acceso.
Estricto	Se puede acceder al host únicamente desde vCenter Server. Si se habilitan SSH o ESXi Shell, se mantienen habilitadas las sesiones en ejecución en las cuentas con la opción avanzada `DCUI.Access` y las cuentas de usuarios con excepción que tienen privilegios de administrador. Todas las demás sesiones se cierran.

6 Haga clic en **Aceptar**.

Deshabilitar el modo de bloqueo

Deshabilite el modo de bloqueo para permitir cambios de configuración en las conexiones directas al host ESXi. Si el modo de bloqueo está habilitado, el entorno es más seguro.

En vSphere 6.0, se puede deshabilitar el modo de bloqueo de la siguiente manera:

Desde la interfaz gráfica de usuario

Los usuarios pueden deshabilitar el modo de bloqueo normal y el modo de bloqueo estricto desde vSphere Client o vSphere Web Client.

Desde la interfaz de usuario de la consola directa

Los usuarios que pueden acceder a la interfaz de usuario de la consola directa en el host ESXi pueden deshabilitar el modo de bloqueo normal. En el modo de bloqueo estricto, el servicio de interfaz de la consola directa se detiene.

Procedimiento

1 Desplácese hasta un host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Perfil de seguridad**.

4 En el panel Modo de bloqueo, haga clic en **Editar**.

5 Haga clic en **Modo de bloqueo** y seleccione **Deshabilitado** para deshabilitar el modo de bloqueo.

6 Haga clic en **Aceptar**.

Resultados

El sistema sale del modo de bloqueo, vCenter Server muestra una alarma y se agrega una entrada al registro de auditoría.

Habilitar o deshabilitar el modo normal de bloqueo desde la interfaz de usuario de la consola directa

Puede habilitar y deshabilitar el modo normal de bloqueo desde la interfaz de usuario de la consola directa (DCUI). El modo de bloqueo estricto puede habilitarse y deshabilitarse únicamente desde vSphere Client o vSphere Web Client.

Cuando el host se encuentra en el modo normal de bloqueo, las siguientes cuentas pueden acceder a la interfaz de usuario de la consola directa:

- Cuentas en la lista de usuarios con excepción que tienen privilegios de administrador en el host. La lista de usuarios con excepción sirve para cuentas de servicios, como un agente de copia de seguridad.
- Usuarios definidos en la opción avanzada `DCUI.Access` del host. Esta opción puede utilizarse para habilitar el acceso en caso de que ocurra un error grave.

En ESXi 6.0 y versiones posteriores, los permisos de usuario se conservan al habilitar el modo de bloqueo. Los permisos de usuario se restauran al deshabilitar el modo de bloqueo desde la interfaz de la consola directa.

Nota Si actualiza un host que se encuentra en el modo de bloqueo a la versión 6.0 de ESXi sin salir de ese modo, y si sale del modo después de actualizar, se perderán todos los permisos definidos antes de que el host entrara en el modo de bloqueo. El sistema asigna la función de administrador a todos los usuarios que se encuentran en la opción avanzada `DCUI.Access` para garantizar el acceso al host.

Para conservar los permisos, deshabilite el modo de bloqueo del host desde vSphere Client o vSphere Web Client antes de realizar la actualización.

Procedimiento

1 En la interfaz de usuario de la consola directa del host, presione F2 e inicie sesión.

2 Desplácese hasta la opción **Configurar el modo de bloqueo** y presione Entrar para alternar la configuración actual.

3 Presione Esc hasta que vuelva al menú principal de la interfaz de usuario de la consola directa.

Especificar cuentas con privilegios de acceso en el modo de bloqueo

Puede especificar cuentas de servicio que puedan acceder al host ESXi. Para ello, agréguelas directamente a la lista de usuarios con excepción. Puede especificar que un único usuario acceda al host ESXi en caso de que se produzca un error grave en vCenter Server.

La versión de vSphere determina qué pueden hacer diferentes cuentas de forma predeterminada cuando se habilita el modo de bloqueo y cómo se puede cambiar el comportamiento predeterminado.

- En vSphere 5.0 y versiones anteriores, únicamente el usuario raíz puede iniciar sesión en la interfaz de usuario de la consola directa (DCUI) en un host ESXi que se encuentra en el modo de bloqueo.
- En vSphere 5.1 y las versiones posteriores, puede agregar un usuario a la configuración avanzada del sistema `DCUI.Access` para cada host. La opción está pensada para un error grave de vCenter Server. Por lo general, las empresas bloquean la contraseña del usuario con este acceso en un lugar seguro. Un usuario de la lista `DCUI.Access` no necesita tener privilegios administrativos completos en el host.
- En vSphere 6.0 y las versiones posteriores, la configuración avanzada del sistema `DCUI.Access` sigue siendo compatible. Asimismo, vSphere 6.0 y las versiones posteriores admiten una lista de usuarios con excepción, destinada a las cuentas de servicio que deben conectarse al host directamente. Las cuentas con privilegios de administrador que figuran en la lista de usuarios con excepción pueden iniciar sesión en ESXi Shell. Por otra parte, estos usuarios pueden iniciar sesión en la DCUI de un host en el modo de bloqueo normal y pueden salir del modo de bloqueo.

Especifique usuarios con excepción desde vSphere Client o vSphere Web Client.

Nota Los usuarios con excepción son usuarios locales del host o usuarios de Active Directory con privilegios definidos localmente para el host ESXi. Los usuarios que son miembros de un grupo de Active Directory pierden sus permisos cuando el host se coloca en modo de bloqueo.

Agregar usuarios a la opción avanzada DCUI.Access

Si se produce un error grave, la opción avanzada `DCUI.Access` permite salir del modo de bloqueo cuando no se puede acceder al host desde vCenter Server. Para agregar usuarios a la lista, edite las opciones de configuración avanzada del host desde vSphere Client.

Nota Los usuarios de la lista de DCUI.Access pueden cambiar la configuración del modo de bloqueo independientemente de los privilegios que tengan. La capacidad de cambiar los modos de bloqueo puede afectar a la seguridad del host. En el caso de las cuentas de servicio que necesitan acceso directo al host, puede ser conveniente agregar usuarios a la lista de usuarios con excepción. Los usuarios con excepción solamente pueden realizar las tareas para las cuales tienen privilegios. Consulte Especificar usuarios con excepción para el modo de bloqueo.

Procedimiento

1. Desplácese hasta el host en el inventario de vSphere Client.
2. Haga clic en **Configurar**.
3. En Sistema, haga clic en **Configuración avanzada del sistema** y en **Editar**.
4. Filtre por DCUI.
5. En el cuadro de texto **DCUI.Access**, introduzca los nombres de usuarios locales de ESXi separados por comas.

   Se incluye al usuario raíz de forma predeterminada. Considere quitar al usuario raíz de la lista de DCUI.Access y especificar una cuenta con nombre para mejorar el proceso de auditoría.
6. Haga clic en **Aceptar**.

Especificar usuarios con excepción para el modo de bloqueo

Puede agregar usuarios a la lista de usuarios con excepción desde vSphere Client. Estos usuarios no pierden sus permisos cuando el host entra en el modo de bloqueo. Por lo tanto, es lógico agregar cuentas de servicio, como un agente de copia de seguridad, a la lista de usuarios con excepción.

Los usuarios con excepción no pierden sus privilegios cuando el host entra en el modo de bloqueo. Es frecuente que estas cuentas representen soluciones y aplicaciones externas que necesitan seguir funcionando en el modo de bloqueo.

Nota La lista de usuarios con excepción no está pensada para administradores sino para las cuentas de servicio que realizan tareas muy específicas. Agregar usuarios administradores a la lista de usuarios con excepción va en contra de la finalidad del modo de bloqueo.

Los usuarios con excepción son usuarios locales del host o usuarios de Active Directory con privilegios definidos localmente para el host ESXi. No son miembros de un grupo de Active Directory y no son usuarios de vCenter Server. Estos usuarios tienen permitido realizar operaciones en el host en función de sus privilegios. Esto significa que, por ejemplo, un usuario con privilegios de solo lectura no puede deshabilitar el modo de bloqueo en un host.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Perfil de seguridad**.

4 En el panel Modo de bloqueo, haga clic en **Editar**.

5 Haga clic en **Usuarios con excepción** y en el icono **Agregar usuario** para agregar usuarios con excepción.

Administrar los niveles de aceptación de hosts y VIB

El nivel de aceptación de un VIB depende de la cantidad de certificaciones de ese VIB. El nivel de aceptación del host depende del nivel del VIB más bajo. Puede cambiar el nivel de aceptación del host si desea permitir VIB de menor nivel. Puede eliminar los VIB CommunitySupported para tener la posibilidad de cambiar el nivel de aceptación del host.

Los VIB son paquetes de software que incluyen una firma de VMware o un partner de VMware. Para conservar la integridad del host ESXi, no permita que los usuarios instalen VIB no firmados (creados por la comunidad). Un VIB no firmado contiene un código no certificado, aceptado ni admitido por VMware o sus partners. Los VIB creados por la comunidad no tienen una firma digital.

El nivel de aceptación del host debe ser igual de restrictivo o menos restrictivo que el nivel de aceptación de cualquier VIB que se desee agregar al host. Por ejemplo, si el nivel de aceptación del host es VMwareAccepted, no se puede instalar VIB en el nivel PartnerSupported. Es posible utilizar los comandos ESXCLI para establecer un nivel de aceptación de un host. Para proteger la seguridad y la integridad de los hosts ESXi, no permita que se instalen VIB no firmados (CommunitySupported) en los hosts de sistemas de producción.

El nivel de aceptación para un host ESXi se muestra en **Perfil de seguridad**, en vSphere Client.

Los siguientes niveles de aceptación son compatibles.

VMwareCertified

El nivel de aceptación VMwareCertified tiene los requisitos más estrictos. Los VIB con este nivel se someten a pruebas completamente equivalentes a las pruebas de control de calidad internas de VMware para la misma tecnología. Hoy en día, solo los controladores de los programas de proveedores de E/S (I/O Vendor Program, IOVP) se publican en este nivel. VMware responde a las llamadas de soporte para VIB con este nivel de aceptación.

VMwareAccepted

Los VIB con este nivel de aceptación pasan por pruebas de comprobación, pero estas no prueban completamente todas las funciones del software. El partner realiza pruebas y VMware comprueba el resultado. Hoy en día, los proveedores de CIM y los complementos de PSA son algunos de los VIB que se publican en este nivel. VMware indica a los clientes que realizan llamadas de soporte para VIB con este nivel de aceptación que se pongan en contacto con la organización de soporte del partner.

PartnerSupported

Los VIB con el nivel de aceptación PartnerSupported los publica un partner de confianza de VMware. El partner realiza todas las pruebas. VMware no comprueba los resultados. Este nivel se utiliza para una tecnología nueva o alternativa que los partners desean habilitar para los sistemas VMware. Hoy en día, las tecnologías de VIB de controlador, como Infiniband, ATAoE y SSD, se encuentran en este nivel con controladores de hardware que no son estándar. VMware indica a los clientes que realizan llamadas de soporte para VIB con este nivel de aceptación que se pongan en contacto con la organización de soporte del partner.

CommunitySupported

El nivel de aceptación CommunitySupported es para VIB creados por personas o empresas por fuera de los programas de partners de VMware. Los VIB de este nivel de aceptación no pasaron por un programa de pruebas aprobado por VMware y no son compatibles con el soporte técnico de VMware ni los partners de VMware.

Procedimiento

1 Conéctese a cada host ESXi y compruebe que el nivel de aceptación esté establecido en VMwareCertified, VMwareAccepted o PartnerSupported con el siguiente comando.

```
esxcli software acceptance get
```

2 Si el nivel de aceptación del host es CommunitySupported, determine si cualquiera de los VIB están en el nivel CommunitySupported con uno de los siguientes comandos.

```
esxcli software vib list
esxcli software vib get -n vibname
```

3 Elimine todos los VIB CommunitySupported con el siguiente comando.

```
esxcli software vib remove --vibname vib
```

4 Cambie el nivel de aceptación del host mediante uno de los siguientes métodos.

Opción	Descripción
Comando de la CLI	`esxcli software acceptance set --level level` El parámetro `level` es obligatorio y especifica el nivel de aceptación que se va a establecer. Debe ser **`VMwareCertified`**, **`VMwareAccepted`**, **`PartnerSupported`** o **`CommunitySupported`**. Consulte *Referencia de ESXCLI* para obtener más información.
vSphere Client	a Seleccione un host en el inventario. b Haga clic en **Configurar**. c En Sistema, seleccione **Perfil de seguridad**. d Haga clic en **Editar** de Nivel de aceptación del perfil de imagen del host y seleccione el nivel de aceptación.

Resultados

El nuevo nivel de aceptación está en vigor.

Nota ESXi realiza comprobaciones de integridad de los VIB regido por el nivel de aceptación. Puede usar la configuración de `VMkernel.Boot.execInstalledOnly` para indicar a ESXi que solo ejecuten archivos binarios que se originen de un VIB válido instalado en el host. Junto con el arranque seguro, esta configuración garantiza que todos los procesos que se ejecuten en ESXi host están firmados, permitidos y esperados. Habilitar esta opción cuando sea posible mejora la seguridad. Para obtener más información sobre la configuración de opciones avanzadas para ESXi, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/kb/1038578.

Asignar privilegios para hosts ESXi

Normalmente, se otorgan privilegios a los usuarios mediante la asignación de permisos para los objetos de los hosts ESXi que administra un sistema vCenter Server. Si se utiliza un host ESXi independiente, se pueden asignar los privilegios directamente.

Asignar permisos para hosts ESXi administrados por vCenter Server

Si el host ESXi está administrado por vCenter Server, realice las tareas de administración a través de vSphere Client.

Puede seleccionar el objeto de host ESXi en la jerarquía de objetos de vCenter Server y asignar la función de administrador a una cantidad limitada de usuarios. Esos usuarios podrán realizar entonces una administración directa en el host ESXi. Consulte Usar funciones para asignar privilegios.

La práctica recomendada implica crear al menos una cuenta de usuario designado, asignarle privilegios administrativos completos en el host y utilizar esta cuenta en lugar de la cuenta raíz. Establezca una contraseña de alta complejidad para la cuenta raíz y limite la utilización de la cuenta raíz. No elimine la cuenta raíz.

Asignar permisos para hosts independientes de ESXi

Se pueden agregar usuarios locales y definir funciones personalizadas desde la pestaña Administración de VMware Host Client. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*.

Para todas las versiones de ESXi, puede ver la lista de usuarios predefinidos en el archivo `/etc/passwd`.

Las siguientes funciones están predefinidas.

Solo lectura

Permite que un usuario vea los objetos asociados con el host ESXi, pero no le permite realizar cambios en los objetos.

Administrador

Función de administrador.

Sin acceso

Sin acceso. Esta función es la función predeterminada. Es posible anular la función predeterminada.

Se pueden administrar grupos y usuarios locales, y agregar funciones locales personalizadas a un host ESXi mediante una instancia de VMware Host Client conectada directamente al host ESXi. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*.

A partir de vSphere 6.0, es posible utilizar los comandos ESXCLI para la administración de cuentas de usuarios locales de ESXi. Los comandos ESXCLI de administración de permisos se pueden utilizar para configurar o quitar permisos tanto en cuentas de Active Directory (usuarios y grupos) como en cuentas locales de ESXi (usuarios únicamente).

Nota Si se define un usuario para el host ESXi mediante una conexión directa al host, y existe un usuario con el mismo nombre en vCenter Server, los usuarios son diferentes. Si se asigna una función al usuario de ESXi, al usuario de vCenter Server no se le asigna la misma función.

Privilegios predefinidos

Si el entorno no incluye un sistema vCenter Server, están predefinidos los siguientes usuarios.

Usuario raíz

Cada host ESXi tiene, de manera predeterminada, una sola cuenta de usuario raíz con la función de administrador. Esa cuenta de usuario raíz puede utilizarse para la administración local y para conectar el host a vCenter Server.

La asignación de privilegios de usuario raíz puede facilitar el ingreso a un host ESXi debido a que el nombre ya se conoce. Tener una cuenta raíz común también dificulta hacer coincidir acciones con usuarios.

Para optimizar la auditoría, cree cuentas individuales con privilegios de administrador. Establezca una contraseña de complejidad alta para la cuenta raíz y limite el uso de la cuenta, por ejemplo, para utilizar en el momento de agregar un host a vCenter Server. No elimine la cuenta raíz. Para obtener más información sobre la asignación de permisos a un usuario para un host ESXi, consulte el documento *Administrar un host único de vSphere: VMware Host Client*.

La práctica recomendada es que todas las cuentas con la función de administrador en un host ESXi se asignen a un usuario específico que tenga una cuenta con nombre. Utilice las funcionalidades de ESXi Active Directory que permiten administrar las credenciales de Active Directory.

Importante Puede quitar los privilegios de acceso al usuario raíz. Sin embargo, primero deberá crear otro permiso a nivel de raíz con otro usuario asignado a la función de administrador.

Usuario vpxuser

vCenter Server utiliza los privilegios del usuario vpxuser cuando se administran actividades del host.

El administrador de vCenter Server puede realizar casi todas las mismas tareas en el host que el usuario raíz y, también, programar tareas, trabajar con plantillas, etc. Sin embargo, el administrador de vCenter Server no puede crear, eliminar o editar usuarios y grupos locales para los hosts de forma directa. Solo un usuario con privilegios de administrador puede realizar estas tareas directamente en un host.

Nota No se puede administrar el usuario vpxuser mediante Active Directory.

Precaución No modifique el usuario vpxuser de ninguna manera. No cambie su contraseña. No cambie sus permisos. Si lo hace, podría experimentar problemas al trabajar con los hosts a través de vCenter Server.

Usuario dcui

El usuario dcui se ejecuta en hosts y actúa con derechos de administrador. El fin principal de este usuario es configurar los hosts para el modo de bloqueo desde la interfaz de usuario de la consola directa (DCUI).

Este usuario actúa como agente para la consola directa, y los usuarios interactivos no pueden modificarlo ni usarlo.

Usar Active Directory para administrar usuarios de ESXi

Se puede configurar ESXi para utilizar un servicio de directorio como Active Directory con el fin de administrar usuarios.

La creación de cuentas de usuarios locales en cada host presenta desafíos para la sincronización de los nombres y las contraseñas de las cuentas en varios hosts. Conecte los hosts ESXi a un dominio de Active Directory para que no sea necesario crear y mantener cuentas de usuarios locales. La utilización de Active Directory para autenticar usuarios simplifica la configuración del host ESXi y reduce el riesgo de que ocurran problemas de configuración que podrían permitir un acceso no autorizado.

Al utilizar Active Directory, los usuarios suministran sus credenciales de Active Directory y el nombre de dominio del servidor de Active Directory cuando se agrega un host a un dominio.

Configurar un host para utilizar Active Directory

Si desea administrar usuarios y grupos, puede configurar un host para el uso de un servicio de directorio como Active Directory.

Cuando agrega un host ESXi en Active Directory, el grupo DOMAIN **ESX Admins** recibe acceso administrativo completo al host si este existe. Si no desea que quede disponible el acceso administrativo completo, consulte el artículo 1025569 de la base de conocimientos de VMware para encontrar una solución alternativa.

Si se aprovisiona un host con Auto Deploy, las credenciales de Active Directory no pueden almacenarse en los hosts. Puede usar vSphere Authentication Proxy para unir el host a un dominio de Active Directory. Dado que existe una cadena de confianza entre vSphere Authentication Proxy y el host, Authentication Proxy puede unir el host al dominio de Active Directory. Consulte Usar vSphere Authentication Proxy.

Nota Al momento de definir la configuración de la cuenta de usuario en Active Directory, es posible definir un límite para los equipos en los que un usuario puede iniciar sesión por el nombre de equipo. De forma predeterminada, no se establecen restricciones similares en una cuenta de usuario. Si se establece dicho límite, las solicitudes de enlaces LDAP de la cuenta de usuario generan errores y muestran el mensaje `Error en el enlace LDAP`, incluso si la solicitud proviene de un equipo que figura en la lista. Para evitar este problema, agregue el nombre netBIOS en el servidor de Active Directory a la lista de equipos en los cuales se puede iniciar sesión con la cuenta de usuario.

Requisitos previos

- Compruebe que tenga un dominio de Active Directory. Consulte la documentación del servidor del directorio.
- Compruebe que el nombre de host ESXi esté completo con el nombre de dominio del bosque de Active Directory.

  fully qualified domain name = host_name.domain_name

Procedimiento

1 Sincronice el tiempo entre ESXi y el sistema de servicio del directorio que utiliza NTP.

   Consulte Sincronización de los relojes de ESXi con un servidor horario de red o la base de conocimientos de VMware para obtener información sobre cómo sincronizar la hora de ESXi con una controladora de dominio de Microsoft.

2 Asegúrese de que los servidores DNS que configuró en el host puedan resolver los nombres de host en las controladoras de Active Directory.

   a Desplácese hasta el host en el inventario de vSphere Client.

   b Haga clic en **Configurar**.

   c En Redes, haga clic en **Configuración de TCP/IP**.

   d En Pila de TCP/IP: Predeterminada, haga clic en **DNS** y compruebe que el nombre de host y la información del servidor DNS del host sean correctos.

Pasos siguientes

Una el host a un dominio de servicio de directorio. Consulte Agregar un host a un dominio de servicio de directorio. En los hosts que se aprovisionan con Auto Deploy, configure vSphere Authentication Proxy. Consulte Usar vSphere Authentication Proxy. Puede configurar permisos para que los usuarios y los grupos del dominio de Active Directory puedan acceder a los componentes de vCenter Server. Para obtener información sobre cómo administrar permisos, consulte Agregar un permiso a un objeto de inventario .

Agregar un host a un dominio de servicio de directorio

Para que el host utilice un servicio de directorio, se debe conectar el host al dominio del servicio de directorio.

Es posible introducir el nombre de dominio con uno de los dos métodos siguientes:

- **`name.tld`** (por ejemplo, **`domain.com`**): la cuenta se crea en el contenedor predeterminado.
- **`name.tld/container/path`** (por ejemplo, **`domain.com/OU1/OU2)`**: la cuenta se crea en una unidad organizativa (OU) en particular.

Para utilizar el servicio vSphere Authentication Proxy, consulte Usar vSphere Authentication Proxy.

Procedimiento

1 Desplácese hasta un host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Servicios de autenticación**.

4 Haga clic en **Unir dominio**.

5 Introduzca un dominio.

   Utilice el formulario **`name.tld`** o **`name.tld/container/path`**.

6 Introduzca el nombre de usuario y la contraseña de un usuario de servicio de directorio que tenga permisos para unir el host al dominio y, a continuación, haga clic en **Aceptar**.

7 (opcional) Si desea utilizar un proxy de autenticación, introduzca la dirección IP del servidor proxy.

8 Haga clic en **Aceptar** para cerrar el cuadro de diálogo Configuración de servicios de directorio.

Pasos siguientes

Puede configurar permisos para que los usuarios y los grupos del dominio de Active Directory puedan acceder a los componentes de vCenter Server. Para obtener información sobre cómo administrar permisos, consulte Agregar un permiso a un objeto de inventario .

Ver la configuración del servicio de directorio

Puede ver el tipo de servidor de directorio (si lo hubiera) que utiliza el host para autenticar usuarios y su respectiva configuración.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Servicios de autenticación**.

   En la página Servicios de autenticación se muestra el servicio del directorio y la configuración del dominio.

Pasos siguientes

Puede configurar permisos para que los usuarios y los grupos del dominio de Active Directory puedan acceder a los componentes de vCenter Server. Para obtener información sobre cómo administrar permisos, consulte Agregar un permiso a un objeto de inventario .

Usar vSphere Authentication Proxy

Se pueden agregar hosts ESXi a un dominio de Active Directory mediante vSphere Authentication Proxy en lugar de agregarlos explícitamente al dominio de Active Directory.

Solo tiene que configurar el host de manera que conozca el nombre de dominio del servidor de Active Directory y la dirección IP de vSphere Authentication Proxy. Cuando vSphere Authentication Proxy está habilitado, automáticamente agrega hosts que se aprovisionan con Auto Deploy al dominio de Active Directory. También puede usar vSphere Authentication Proxy con hosts que no se aprovisionan mediante Auto Deploy.

Consulte Puertos necesarios para vCenter Server y Platform Services Controller para obtener información sobre los puertos TCP que emplea vSphere Authentication Proxy.

Auto Deploy

Si aprovisiona hosts con Auto Deploy, puede configurar un host de referencia que apunte a Authentication Proxy. A continuación, debe configurar una regla que aplique el perfil del host de referencia a cualquier host ESXi que esté aprovisionado con Auto Deploy. vSphere Authentication Proxy almacena las direcciones IP de todos los hosts que Auto Deploy aprovisiona mediante PXE en la lista de control de acceso. Cuando el host arranca, se pone en contacto con vSphere Authentication Proxy, el cual une esos hosts, que ya están en la lista de control de acceso, al dominio de Active Directory.

Incluso si usa vSphere Authentication Proxy en un entorno que utiliza certificados aprovisionados por VMCA o certificados de terceros, el proceso funciona sin problemas si sigue las instrucciones para usar certificados personalizados con Auto Deploy.

Consulte Usar certificados personalizados con Auto Deploy.

Otros hosts ESXi

Se pueden configurar otros hosts para que usen vSphere Authentication Proxy si desea permitir que el host se una al dominio sin usar credenciales de Active Directory. Es decir, no necesita transmitir credenciales de Active Directory al host ni guardar credenciales de Active Directory en el perfil de host.

En ese caso, debe agregar la dirección IP del host a la lista de control de acceso de vSphere Authentication Proxy para que este autorice el host según su dirección IP predeterminada. Puede habilitar la autenticación del cliente para que vSphere Authentication Proxy realice la verificación del certificado del host.

Nota No se puede utilizar vSphere Authentication Proxy en un entorno compatible solo con IPv6.

Habilitar vSphere Authentication Proxy

El servicio vSphere Authentication Proxy se encuentra disponible en cada sistema de vCenter Server. De forma predeterminada, el servicio no se encuentra en ejecución. Si desea usar vSphere Authentication Proxy en el entorno, puede iniciar el servicio desde la interfaz de administración de vCenter Server Appliance, desde vSphere Web Client o desde la línea de comandos.

El servicio de vSphere Authentication Proxy se enlaza a una dirección IPv4 para comunicarse con vCenter Server y no admite IPv6. La instancia de vCenter Server puede residir en un equipo host de un entorno de red de solo IPv4 o de modo mixto IPv4/IPv6. Sin embargo, cuando se especifica la dirección de vSphere Authentication Proxy, se debe especificar una dirección IPv4.

Requisitos previos

Compruebe que utiliza vCenter Server 6.5 o de una versión posterior. En las versiones anteriores de vSphere, vSphere Authentication Proxy se instala por separado. Consulte la documentación de la versión anterior del producto para obtener instrucciones.

Procedimiento

1 Inicie el servicio de VMware vSphere Authentication Proxy.

Opción	Descripción
Interfaz de administración de vCenter Server Appliance (VAMI)	a En un explorador web, vaya a la interfaz de administración de vCenter Server Appliance, https://*dirección-IP-o-FQDN-de-dispositivo*:5480. b Inicie sesión como raíz. La contraseña raíz predeterminada es la que estableció al implementar vCenter Server Appliance. c Haga clic en **Servicios** y en el servicio **VMware vSphere Authentication Proxy**. d Haga clic en **Iniciar**.
vSphere Web Client	a Haga clic en **Administración** y en **Configuración del sistema** en **Implementación**. b Haga clic en **Servicios** y en el servicio **VMware vSphere Authentication Proxy**. c Haga clic en el icono verde **Iniciar el servicio** en la barra de menús de la parte superior de la ventana. d (Opcional) Una vez iniciado el servicio, haga clic en **Acciones > Editar tipo de inicio** y seleccione **Automático** para que el inicio sea automático.

2 Confirme que el servicio se inició correctamente.

Resultados

A continuación, se podrá establecer el dominio de vSphere Authentication Proxy. Después de eso, vSphere Authentication Proxy controlará todos los hosts aprovisionados con Auto Deploy y el usuario podrá agregar hosts de forma explícita a vSphere Authentication Proxy.

Agregar un dominio a vSphere Authentication Proxy con vSphere Web Client

Puede agregar un dominio a vSphere Authentication Proxy desde vSphere Web Client o con el comando `camconfig`.

Puede agregar un dominio en vSphere Authentication Proxy únicamente después de habilitar el proxy. Después de agregar el dominio, vSphere Authentication Proxy agrega todos los hosts que se aprovisionan con Auto Deploy en ese dominio. En los demás hosts, también puede utilizar vSphere Authentication Proxy si no desea otorgar privilegios de dominio para esos hosts.

Procedimiento

1 Conéctese a un sistema vCenter Server con vSphere Web Client.

2 Haga clic en **Administración** y en **Configuración del sistema** en **Implementación**.

3 Haga clic en **Servicios**, en el servicio **VMware vSphere Authentication Proxy** y, a continuación, en **Editar**.

4 Introduzca el nombre del dominio al que vSphere Authentication Proxy agregará los hosts y el nombre de un usuario con privilegios de Active Directory para agregar hosts al dominio.

   Los otros campos en este cuadro de diálogo tienen fines meramente informativos.

5 Haga clic en el icono de puntos suspensivos para agregar y confirmar la contraseña del usuario y, a continuación, haga clic en **Aceptar**.

Agregar un dominio a vSphere Authentication Proxy con el comando camconfig

Puede agregar un dominio a vSphere Authentication desde vSphere Web Client o con el comando `camconfig`.

Puede agregar un dominio en vSphere Authentication Proxy únicamente después de habilitar el proxy. Después de agregar el dominio, vSphere Authentication Proxy agrega todos los hosts que se aprovisionan con Auto Deploy en ese dominio. En los demás hosts, también puede utilizar vSphere Authentication Proxy si no desea otorgar privilegios de dominio para esos hosts.

Procedimiento

1 Inicie sesión en el dispositivo vCenter Server o en el equipo vCenter Server Windows como usuario con privilegios de administrador.

2 Ejecute el comando para habilitar el acceso al shell de Bash.

```
shell
```

3 Desplácese hasta el directorio en donde se encuentra el script **camconfig**.

Sistema operativo	Ubicación
Dispositivo vCenter Server	`/usr/lib/vmware-vmcam/bin/`
vCenter Server Windows	`C:\Archivos de programa\VMware\vCenter Server\vmcamd\`

4 Para agregar las credenciales de usuario y de dominio de Active Directory a la configuración de Authentication Proxy, ejecute el siguiente comando.

```
camconfig add-domain -d domain -u user
```

   Se le solicita una contraseña.

   vSphere Authentication Proxy almacena ese nombre de usuario y esa contraseña en la memoria caché. Puede eliminar y volver a crear el usuario según se requiera. Debe ser posible acceder al dominio a través de DNS, pero no es necesario que sea un origen de identidad de vCenter Single Sign-On.

vSphere Authentication Proxy usa el nombre de usuario especificado por *user* para crear las cuentas de los hosts ESXi en Active Directory. El usuario debe tener privilegios para crear cuentas en el dominio de Active Directory al que se desea añadir los hosts. Al momento de escribir esta información, el artículo 932455 de Microsoft Knowledge Base brinda información complementaria sobre los privilegios de creación de cuentas.

5 Si más adelante desea eliminar la información de dominio y usuario de vSphere Authentication Proxy, ejecute el siguiente comando.

```
camconfig remove-domain -d domain
```

Usar vSphere Authentication Proxy para agregar un host a un dominio

El servidor Auto Deploy agrega todos los hosts que aprovisiona a vSphere Authentication Proxy, que agrega esos hosts al dominio. Si desea utilizar vSphere Authentication Proxy para agregar otros hosts a un dominio, puede agregarlos a vSphere Authentication Proxy explícitamente. A continuación, el servidor vSphere Authentication Proxy agrega esos hosts al dominio. Como resultado, ya no es necesario que las credenciales suministradas por el usuario sean transmitidas al sistema de vCenter Server.

Es posible introducir el nombre de dominio con uno de los dos métodos siguientes:

- **`name.tld`** (por ejemplo, **`domain.com`**): la cuenta se crea en el contenedor predeterminado.
- **`name.tld/container/path`** (por ejemplo, **`domain.com/OU1/OU2)`**: la cuenta se crea en una unidad organizativa (OU) en particular.

Requisitos previos

- Si el host ESXi está utilizando un certificado firmado por VMCA, compruebe que el host se haya agregado a vCenter Server. De lo contrario, el servicio de Authentication Proxy no puede confiar en el host ESXi.
- Si el host ESXi está utilizando un certificado firmado por una entidad de certificación raíz, compruebe que se haya agregado el certificado firmado por la CA raíz correspondiente al sistema de vCenter Server. Consulte Administrar certificados para hosts ESXi.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En **Sistema**, seleccione **Servicios de autenticación**.

4 Haga clic en **Unir dominio**.

5 Introduzca un dominio.

Utilice el formato **`name.tld`**, por ejemplo **`midominio.com`**, o **`name.tld/container/path`**, por ejemplo, **`midominio.com/organizational_unit1/organizational_unit2`**.

6 Seleccione **Utilizar servidor proxy**.

7 Introduzca la dirección IP del servidor Authentication Proxy, que siempre es la misma que la dirección IP del sistema de vCenter Server.

8 Haga clic en **Aceptar**.

Habilitar la autenticación de cliente para vSphere Authentication Proxy

De forma predeterminada, vSphere Authentication Proxy agrega todo host que posea una dirección IP incluida en su lista de control de acceso. Para aumentar la seguridad, es posible habilitar la autenticación de cliente. Si se habilita la autenticación de cliente, vSphere Authentication Proxy también comprueba el certificado del host.

Requisitos previos

- Compruebe que el sistema vCenter Server confíe en el host. De forma predeterminada, cuando se agrega un host a vCenter Server, se asigna al host un certificado con la firma de una entidad de certificación raíz de confianza de vCenter Server. vSphere Authentication Proxy confía en la entidad de certificación raíz de confianza de vCenter Server.
- Si planea reemplazar los certificados de ESXi en el entorno, realice el reemplazo antes de habilitar vSphere Authentication Proxy. Los certificados en el host ESXi deben coincidir con los del registro del host.

Procedimiento

1 Inicie sesión en el dispositivo vCenter Server o en el equipo vCenter Server Windows como usuario con privilegios de administrador.

2 Ejecute el comando para habilitar el acceso al shell de Bash.

```
shell
```

3 Desplácese hasta el directorio en donde se encuentra el script **camconfig**.

Sistema operativo	Ubicación
Dispositivo vCenter Server	`/usr/lib/vmware-vmcam/bin/`
vCenter Server Windows	`C:\Archivos de programa\VMware\vCenter Server\vmcamd\`

4 Ejecute el siguiente comando para habilitar la autenticación de cliente.

```
camconfig ssl-cliAuth -e
```

En adelante, vSphere Authentication Proxy comprobará el certificado de cada host que se agregue.

5 Si posteriormente desea volver a deshabilitar la autenticación de cliente, ejecute el siguiente comando.

```
camconfig ssl-cliAuth -n
```

Importar el certificado de vSphere Authentication Proxy en el host ESXi

De manera predeterminada, los hosts ESXi requieren la comprobación explícita del certificado de vSphere Authentication Proxy. Si usa vSphere Auto Deploy, el servicio de Auto Deploy se ocupa de agregar el certificado a los hosts que aprovisiona. Para otros hosts, el certificado se debe agregar de forma explícita.

Requisitos previos

- Cargue el certificado de vSphere Authentication Proxy en un almacén de datos accesible para el host ESXi. Mediante una aplicación SFTP como WinSCP, puede descargar el certificado del host de vCenter Server en la siguiente ubicación.

  vCenter Server Appliance

  `/var/lib/vmware/vmcam/ssl/rui.crt`

  vCenter Server en Windows

  `C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt`

- Compruebe que la configuración avanzada de `UserVars.ActiveDirectoryVerifyCAMCertificate`ESXi esté establecida en 1 (valor predeterminado).

Procedimiento

1 Seleccione el host ESXi y haga clic en **Configurar**.

2 En **Sistema**, seleccione **Servicios de autenticación**.

3 Haga clic en **Importar certificado**.

4 Introduzca la ruta de acceso al archivo de certificado siguiendo el formato `[`*`datastore`*`]/`*`path`*`/`*`certname`*`.crt` y, a continuación, haga clic en **Aceptar**.

Generar un nuevo certificado para vSphere Authentication Proxy

Si desea generar un nuevo certificado aprovisionado por la VMCA o un nuevo certificado que incluya a la VMCA como certificado subordinado, siga los pasos detallados en este tema.

Consulte Configurar vSphere Authentication Proxy para usar certificados personalizados si desea usar un certificado que esté firmado por una entidad de certificación externa o empresarial.

Requisitos previos

Debe tener privilegios de raíz o de administrador sobre el sistema en el que se ejecuta vSphere Authentication Proxy.

Procedimiento

1 Haga una copia de `certool.cfg`.

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2 Edite la copia con alguna información de su organización, como en el ejemplo siguiente.

```
Country = IE
Name = vmcam
Organization = VMware
OrgUnit = vTSU
State = Cork
Locality = Cork
Hostname = test-cam-1.test1.vmware.com
```

3 Genere la nueva clave privada en `/var/lib/vmware/vmcam/ssl/`.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=/var/lib/vmware/vmcam/ssl/rui.key --
pubkey=/tmp/vmcam.pub --server=localhost
```

Para *localhost*, suministre el FQDN de Platform Services Controller.

4 Genere el nuevo certificado en `/var/lib/vmware/vmcam/ssl/` usando la clave y el archivo `vmcam.cfg` que creó en el paso 1 y el paso 2.

```
/usr/lib/vmware-vmca/bin/certool --server=localhost --gencert --privkey=/var/lib/
vmware/vmcam/ssl/rui.key --cert=/var/lib/vmware/vmcam/ssl/rui.crt --config=/var/lib/vmware/
vmcam/ssl/vmcam.cfg
```

Para *localhost*, suministre el FQDN de Platform Services Controller.

Configurar vSphere Authentication Proxy para usar certificados personalizados

El uso de certificados personalizados con vSphere Authentication Proxy consta de varios pasos. Primero, genere una CSR y envíela a la entidad de certificación para que la firme. A continuación, coloque el certificado firmado y el archivo de clave en una ubicación a la que vSphere Authentication Proxy pueda acceder.

De manera predeterminada, vSphere Authentication Proxy genera una CSR durante el primer arranque y pide a VMCA que firme esa CSR. vSphere Authentication Proxy se registra con vCenter Server y usa ese certificado. Puede usar certificados personalizados en el entorno si los agrega a vCenter Server.

Procedimiento

1 Genere una CSR para vSphere Authentication Proxy.

   a Cree un archivo de configuración, `/var/lib/vmware/vmcam/ssl/vmcam.cfg`, como se muestra en el siguiente ejemplo.

```
[ req ]
distinguished_name = req_distinguished_name
encrypt_key = no
prompt = no
string_mask = nombstr
req_extensions = v3_req
[ v3_req ]
basicConstraints = CA:false
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = DNS:dns.static-1.csl.vmware.com
[ req_distinguished_name ]
countryName = IE
stateOrProvinceName = Cork
localityName = Cork
0.organizationName = VMware
organizationalUnitName = vTSU
commonName = test-cam-1.test1.vmware.com
```

   b Ejecute `openssl` para generar un archivo CSR y un archivo de claves, pasando el archivo de configuración.

```
openssl req -new -nodes -out vmcam.csr -newkey rsa:2048 -keyout /var/lib/vmware/
vmcam/ssl/rui.key -config /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2 Realice una copia de seguridad del certificado `rui.crt` y de los archivos `rui.key`, que están almacenados en la siguiente ubicación.

Sistema operativo	Ubicación
vCenter Server Appliance	`/var/lib/vmware/vmcam/ssl/rui.crt`
vCenter Server en Windows	`C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt`

3 Elimine vSphere Authentication Proxy del registro.

   a Desplácese hasta el directorio en donde se ubica el script de `camregister`.

Sistema operativo	Comandos
vCenter Server Appliance	`/usr/lib/vmware-vmcam/bin`
vCenter Server en Windows	`C:\Archivos de programa\VMware\vCenter Server\vmcamd`

   b Ejecute el siguiente comando.

```
camregister --unregister -a VC_address -u user
```

   El valor *user* debe ser un usuario de vCenter Single Sign-On que tenga permisos de administrador en vCenter Server.

4 Detenga el servicio de vSphere Authentication Proxy.

Herramienta	Pasos
Interfaz de administración de vCenter Server Appliance (VAMI)	a En un explorador web, vaya a la interfaz de administración de vCenter Server Appliance, https://*dirección-IP-o-FQDN-de-dispositivo*:5480. b Inicie sesión como usuario root. La contraseña raíz predeterminada es la que estableció al implementar vCenter Server Appliance. c Haga clic en **Servicios** y en el servicio **VMware vSphere Authentication Proxy**. d Haga clic en **Detener**.
vSphere Web Client	a Seleccione **Administración** y haga clic en **Configuración del sistema** en **Implementación**. b Haga clic en **Servicios**, en el servicio de **VMware vSphere Authentication Proxy** y en el icono rojo **Detener el servicio**.
CLI	`service-control --stop vmcam`

5 Reemplace el certificado `rui.crt` existente y los archivos `rui.key` por los archivos que le envió la entidad de certificación.

6 Reinicie el servicio de vSphere Authentication Proxy.

7 Vuelva a registrar vSphere Authentication Proxy explícitamente en vCenter Server usando el nuevo certificado y la clave.

```
camregister --register -a VC_address -u user -c full_path_to_rui.crt -k
full_path_to_rui.key
```

Configurar la autenticación de tarjeta inteligente de ESXi

Se puede utilizar la autenticación de tarjeta inteligente para iniciar sesión en la interfaz de usuario de la consola directa (Direct Console User Interface, DCUI) de ESXi mediante la comprobación

de identidad personal (Personal Identity Verification, PIV), la tarjeta de acceso común (Common Access Card, CAC) o la tarjeta inteligente SC650, en lugar de especificar un nombre de usuario y una contraseña.

Una tarjeta inteligente es una tarjeta plástica pequeña con un chip de circuito integrado. Muchas agencias gubernamentales y empresas grandes utilizan la autenticación en dos fases basada en tarjeta inteligente para incrementar la seguridad de los sistemas y cumplir con las normas de seguridad.

Cuando se habilita la autenticación de tarjeta inteligente en un host ESXi, la DCUI solicita una combinación de tarjeta inteligente y PIN, en lugar de la solicitud predeterminada de nombre de usuario y contraseña.

1. Cuando se introduce la tarjeta inteligente en el lector de tarjetas inteligentes, el host ESXi lee las credenciales de la tarjeta.
2. La DCUI de ESXi muestra su identificador de inicio de sesión y solicita su PIN.
3. Una vez introducido el PIN, el host ESXi busca coincidencias con el PIN almacenado en la tarjeta inteligente y comprueba el certificado en la tarjeta inteligente con Active Directory.
4. Después de la correcta comprobación del certificado de la tarjeta inteligente, ESXi inicia su sesión en la DCUI.

Para pasar a la autenticación mediante nombre de usuario y contraseña desde la DCUI, presione F3.

El chip de la tarjeta inteligente se bloquea después de una serie de ingresos de PIN incorrecto; por lo general, después de tres intentos. Si se bloquea la tarjeta inteligente, únicamente el personal designado puede desbloquearla.

Habilitar la autenticación de tarjeta inteligente

Habilite la autenticación de tarjeta inteligente para que el sistema solicite la combinación de tarjeta inteligente y PIN para iniciar sesión en la DCUI de ESXi.

Requisitos previos

- Configure la infraestructura para que controle la autenticación de tarjeta inteligente, como cuentas del dominio de Active Directory, lectores de tarjetas inteligentes y tarjetas inteligentes.
- Configure ESXi para que se una a un dominio de Active Directory que admita la autenticación de tarjeta inteligente. Para obtener más información, consulte Usar Active Directory para administrar usuarios de ESXi.
- Utilice vSphere Client para agregar certificados raíz. Consulte Administrar certificados para hosts ESXi.

Procedimiento

1. Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Servicios de autenticación**.

   Puede ver el estado actual de autenticación de tarjeta inteligente y una lista con los certificados importados.

4 En el panel Autenticación de tarjeta inteligente, haga clic en **Editar**.

5 En el cuadro de diálogo Editar autenticación de tarjeta inteligente, seleccione la página Certificados.

6 Agregue certificados de una entidad de certificación (CA) de confianza, por ejemplo, certificados de una CA raíz o intermediaria.

   Los certificados deben estar en formato PEM.

7 Abra la página Autenticación de tarjeta inteligente, active la casilla **Habilitar autenticación de tarjeta inteligente** y haga clic en **Aceptar**.

Deshabilitar la autenticación de tarjeta inteligente

Deshabilite la autenticación de tarjeta inteligente para regresar a la autenticación predeterminada de nombre de usuario y contraseña que permite iniciar sesión en la DCUI de ESXi.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Servicios de autenticación**.

   Puede ver el estado actual de autenticación de tarjeta inteligente y una lista con los certificados importados.

4 En el panel Autenticación de tarjeta inteligente, haga clic en **Editar**.

5 En la página Autenticación de tarjeta inteligente, desactive la casilla **Habilitar autenticación de tarjeta inteligente** y haga clic en **Aceptar**.

Autenticar con nombre de usuario y contraseña en caso de problemas de conectividad

Si no se puede tener acceso al servidor de dominios de Active Directory (AD), puede iniciar sesión en la DCUI de ESXi con la autenticación de nombre de usuario y contraseña para realizar acciones de emergencia en el host.

En raras ocasiones, no se puede tener acceso al servidor de dominio de AD para autenticar las credenciales de usuario en la tarjeta inteligente debido a problemas de conectividad, cortes de red o desastres. En ese caso, puede iniciar sesión en el DCUI de ESXi con las credenciales de un usuario administrador de ESXi local. Después de iniciar sesión, puede realizar diagnósticos u otras acciones de emergencia. La reserva del inicio de sesión con nombre de usuario y contraseña queda registrada. Cuando la conectividad a AD se restaura, se vuelve a habilitar la autenticación de tarjeta inteligente.

Nota La pérdida de la conectividad de red con vCenter Server no afecta la autenticación de tarjeta inteligente si el servidor de Active Directory (AD) está disponible.

Usar la autenticación de tarjeta inteligente en el modo de bloqueo

Cuando el modo de bloqueo está habilitado en el host ESXi, aumenta la seguridad del host y se limita el acceso a la interfaz de usuario de la consola directa (DCUI). El modo de bloqueo puede deshabilitar la característica de autenticación de tarjeta inteligente.

En el modo normal de bloqueo, únicamente los usuarios que figuran en la lista de usuarios con excepción con privilegios de administrador pueden acceder a la DCUI. Los usuarios con excepción son usuarios locales del host o usuarios de Active Directory con permisos definidos localmente para el host ESXi. Si desea utilizar la autenticación de tarjeta inteligente en el modo de bloqueo normal, debe agregar usuarios a la lista de usuarios con excepción desde vSphere Client. Estos usuarios no pierden sus permisos cuando el host entra en el modo de bloqueo normal y pueden iniciar sesión en la DCUI. Para obtener más información, consulte Especificar usuarios con excepción para el modo de bloqueo.

En el modo de bloqueo estricto, el servicio de la DCUI se interrumpe. Como consecuencia, no se puede acceder al host con la autenticación de tarjeta inteligente.

Usar ESXi Shell

ESXi Shell está deshabilitado de manera predeterminada en los hosts ESXi. Es posible habilitar el acceso local y remoto al shell, si es necesario.

Para reducir el riesgo de accesos no autorizados, habilite ESXi Shell solo para solucionar problemas.

ESXi Shell es independiente del modo de bloqueo. Incluso si el host se ejecuta en modo de bloqueo, todavía puede iniciar sesión en ESXi Shell si está habilitado.

ESXi Shell

Habilite este servicio para acceder a ESXi Shell de forma local.

SSH

Habilite este servicio para acceder a ESXi Shell de forma remota mediante SSH.

El usuario raíz y los usuarios con la función de administrador pueden acceder a ESXi Shell. Los usuarios que se encuentran en el grupo de Administradores de ESX reciben automáticamente la función de administrador. De forma predeterminada, solamente el usuario raíz puede ejecutar comandos del sistema (como `vmware -v`) mediante ESXi Shell.

Nota No habilite ESXi Shell a menos que necesite el acceso.

- Habilitar el acceso a ESXi Shell

  Puede utilizar vSphere Client o vSphere Web Client para habilitar el acceso local o remoto (SSH) a ESXi Shell, y para establecer el tiempo de espera de inactividad y de disponibilidad.

- Usar la interfaz de usuario de la consola directa para habilitar el acceso a ESXi Shell

  La interfaz de usuario de la consola directa (DCUI) permite interactuar con el host de forma local mediante los menús basados en texto. Determine si los requisitos de seguridad de su entorno admiten la habilitación de la interfaz de usuario de la consola directa.

- Iniciar sesión en ESXi Shell para solucionar problemas

  Realice las tareas de configuración de ESXi con vSphere Client, vSphere CLI o vSphere PowerCLI. Inicie sesión en ESXi Shell (anteriormente Tech Support Mode o TSM) solo para fines de solución de problemas.

Habilitar el acceso a ESXi Shell

Puede utilizar vSphere Client o vSphere Web Client para habilitar el acceso local o remoto (SSH) a ESXi Shell, y para establecer el tiempo de espera de inactividad y de disponibilidad.

Nota Acceda al host con vSphere Web Client, las herramientas remotas de línea de comandos (vCLI y PowerCLI) y las API publicadas. No habilite el acceso remoto al host con SSH a menos que se presenten circunstancias especiales que requieran que habilite el acceso de SSH.

Requisitos previos

Si desea utilizar una clave de SSH autorizada, puede cargarla. Consulte Claves SSH de ESXi.

Procedimiento

1 Desplácese hasta el host en el inventario.

2 Desplácese hasta el panel Servicios.

Opción	Descripción
vSphere Client	a Haga clic en **Configurar**. b En Sistema, haga clic en **Servicios**.
vSphere Web Client	a Haga clic en **Configurar**. b En Sistema, haga clic en **Perfil de seguridad**.

3 Administre los servicios de ESXi, SSH o interfaz de usuario de consola directa.

Opción	Descripción
vSphere Client	a En el panel Servicios, seleccione el servicio. b Haga clic en **Editar directiva de inicio** y seleccione la directiva de inicio **Iniciar y detener manualmente**. c Para habilitar el servicio, haga clic en **Iniciar**.
vSphere Web Client	a En el panel Servicios, haga clic en **Editar**. b Haga clic en **Detalles de servicio** y seleccione la directiva de inicio **Iniciar y detener manualmente**. c Para habilitar el servicio, haga clic en **Iniciar**. d Haga clic en **Aceptar**.

Cuando se selecciona **Iniciar y detener manualmente**, el servicio no se inicia al reiniciar el host. Si desea que el servicio se inicie al reiniciar el host, seleccione **Iniciar y detener con el host**.

Pasos siguientes

Establezca los tiempos de espera de disponibilidad e inactividad para ESXi Shell. Consulte Crear un tiempo de espera de disponibilidad de ESXi Shell y Crear un tiempo de espera para sesiones de ESXi Shell inactivas.

Crear un tiempo de espera de disponibilidad de ESXi Shell

La instancia de ESXi Shell está deshabilitada de forma predeterminada. Puede establecer un tiempo de espera de disponibilidad para ESXi Shell a fin de aumentar la seguridad cuando se habilita el shell.

La configuración de tiempo de espera de disponibilidad corresponde a la cantidad de tiempo que puede transcurrir antes de que pueda iniciar sesión tras la habilitación de ESXi Shell. Una vez que transcurre el período de espera, el servicio se deshabilita y los usuarios no pueden iniciar sesión.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Configuración avanzada del sistema**.

4 Haga clic en **Editar** y seleccione `UserVars.ESXiShellTimeOut`.

5 Introduzca la configuración de tiempo de espera de inactividad.

   Debe reiniciar el servicio SSH y el servicio ESXi Shell para que se aplique el tiempo de espera.

6 Haga clic en **Aceptar**.

Resultados

Si inicia sesión y se agota el tiempo de espera, la sesión se mantiene activa. No obstante, una vez que se cierra o se interrumpe la sesión, los usuarios no pueden iniciar sesión.

Crear un tiempo de espera para sesiones de ESXi Shell inactivas

Si habilita ESXi Shell en un host, pero olvida cerrar la sesión, la sesión inactiva permanece conectada de forma indefinida. La conexión abierta aumenta las posibilidades de que alguien obtenga acceso privilegiado al host. Para impedir esta situación, configure un tiempo de espera para las sesiones inactivas.

El tiempo de espera de inactividad corresponde a la cantidad de tiempo que puede transcurrir antes de que se cierre la sesión interactiva inactiva de un usuario. Es posible controlar la cantidad de tiempo que duran una sesión local y una sesión remota (SSH) desde la interfaz de usuario de la consola directa (DCUI) o desde vSphere Client.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.
2 Haga clic en **Configurar**.
3 En Sistema, seleccione **Configuración avanzada del sistema**.
4 Haga clic en **Editar**, seleccione `UserVars.ESXiShellInteractiveTimeOut` e introduzca la configuración de tiempo de espera.

   Un valor de cero (0) deshabilita el tiempo de inactividad.
5 Reinicie el servicio de ESXi Shell y el servicio SSH para que se aplique el tiempo de espera.

Resultados

Si la sesión está inactiva, se cerrará la sesión de los usuarios una vez transcurrido el período de tiempo de espera.

Usar la interfaz de usuario de la consola directa para habilitar el acceso a ESXi Shell

La interfaz de usuario de la consola directa (DCUI) permite interactuar con el host de forma local mediante los menús basados en texto. Determine si los requisitos de seguridad de su entorno admiten la habilitación de la interfaz de usuario de la consola directa.

Se puede utilizar la interfaz de usuario de la consola directa (DCUI) para habilitar el acceso local o remoto a ESXi Shell. A la interfaz de usuario de la consola directa se accede desde la consola física asociada al host. Después de que el host se reinicie y cargue ESXi, pulse F2 para iniciar sesión en la DCUI. Introduzca las credenciales que creó cuando instaló ESXi.

Nota Los cambios que se realizan en el host desde la interfaz de usuario de la consola directa, vSphere Client, ESXCLI u otras herramientas administrativas se envían al almacenamiento permanente cada una hora o después de un apagado correcto. Si se produce un error en el host antes de que los cambios se confirmen, estos podrían perderse.

Procedimiento

1 En la interfaz de usuario de la consola directa, presione F2 para acceder al menú Personalización del sistema.

2 Seleccione **Opciones de solución de problemas** y presione Intro.

3 En el menú Opciones del modo de solución de problemas, seleccione un servicio para habilitar.

   - Habilitar ESXi Shell
   - Habilitar SSH

4 Presione Intro para habilitar el servicio.

5 Presione Esc hasta que vuelva al menú principal de la interfaz de usuario de la consola directa.

Pasos siguientes

Establezca los tiempos de espera de disponibilidad e inactividad para ESXi Shell. Consulte Establecer el tiempo de espera de disponibilidad o el tiempo de espera de inactividad para ESXi Shell.

Establecer el tiempo de espera de disponibilidad o el tiempo de espera de inactividad para ESXi Shell

La instancia de ESXi Shell está deshabilitada de forma predeterminada. Para aumentar la seguridad cuando se habilita el shell, puede establecer un tiempo de espera de disponibilidad, un tiempo de espera de inactividad o ambos.

Los dos tipos de tiempo de espera se aplican en situaciones diferentes.

Tiempo de espera de inactividad

Si un usuario habilita ESXi Shell en un host, pero olvida cerrar la sesión, la sesión inactiva permanece conectada de forma indefinida. La conexión abierta puede aumentar la posibilidad de que alguien obtenga acceso privilegiado al host. Para evitar que esta situación se produzca, configure un tiempo de espera de las sesiones inactivas.

Tiempo de espera de disponibilidad

El tiempo de espera de disponibilidad determina cuánto tiempo puede transcurrir antes de iniciar sesión después de habilitar el shell inicialmente. Si espera más tiempo, el servicio se deshabilita y ya no se puede iniciar sesión en ESXi Shell.

Requisitos previos

Habilite ESXi Shell. Consulte Usar la interfaz de usuario de la consola directa para habilitar el acceso a ESXi Shell.

Procedimiento

1 Inicie sesión en ESXi Shell.

2 En el menú Opciones del modo de solución de problemas, seleccione **Modificar tiempos de espera de SSH y ESXi Shell** y presione Intro.

3 Introduzca el tiempo de espera de inactividad (en segundos) o el tiempo de espera de disponibilidad.

   Debe reiniciar el servicio SSH y el servicio ESXi Shell para que se aplique el tiempo de espera.

4 Presione Entrar y Esc hasta regresar al menú principal de la interfaz de usuario de la consola directa.

5 Haga clic en **Aceptar**.

Resultados

- Si establece el tiempo de espera de inactividad, se desconecta a los usuarios una vez que la sesión está inactiva durante el tiempo especificado.
- Si establece el tiempo de espera de disponibilidad y no inicia sesión antes de que transcurra ese tiempo de espera, los inicios de sesión se vuelven a deshabilitar.

Iniciar sesión en ESXi Shell para solucionar problemas

Realice las tareas de configuración de ESXi con vSphere Client, vSphere CLI o vSphere PowerCLI. Inicie sesión en ESXi Shell (anteriormente Tech Support Mode o TSM) solo para fines de solución de problemas.

Procedimiento

1 Inicie sesión en ESXi Shell con uno de los siguientes métodos.

   - Si tiene acceso directo al host, presione Alt + F1 para abrir la página de inicio de sesión en la consola física de la máquina.
   - Si se conecta al host de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en el host.

2 Escriba un nombre de usuario y una contraseña que reconozca el host.

Arranque seguro UEFI para hosts ESXi

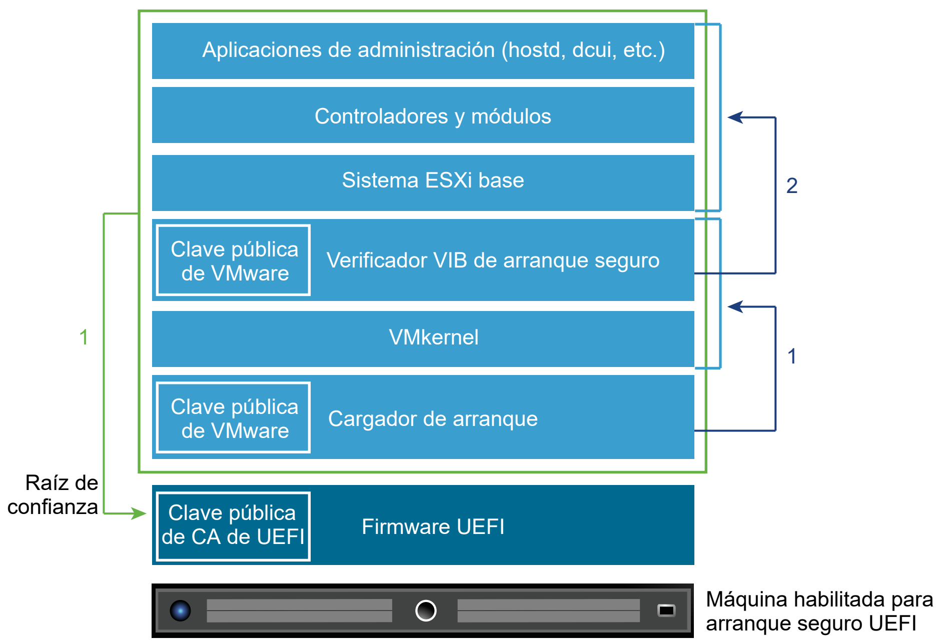
El arranque seguro forma parte del estándar de firmware UEFI. Con el arranque seguro habilitado, una máquina se niega a cargar cualquier controlador UEFI o aplicación, salvo que el cargador de arranque del sistema operativo esté firmado con datos de cifrado. A partir de vSphere 6.5, ESXi admite el arranque seguro si está habilitado en el hardware.

descripción general de arranque seguro UEFI

ESXi 6.5 y las versiones posteriores admiten el arranque seguro UEFI en cada nivel de la pila de arranque.

Nota Antes de usar el arranque seguro UEFI en un host que se haya actualizado a ESXi 6.5, siga las instrucciones en Ejecutar el script de validación de arranque seguro en un host ESXi actualizado para verificar la compatibilidad. Si actualiza un host ESXi mediante los comandos `esxcli`, la actualización no actualiza el cargador de arranque. En ese caso, no podrá realizar un arranque seguro en ese sistema.

Figura 3-1. arranque seguro UEFI



Con el arranque seguro habilitado, la secuencia de arranque es la que se describe a continuación.

1 A partir de vSphere 6.5, el cargador de arranque de ESXi contiene una clave pública de VMware. El cargador de arranque utiliza la clave para verificar la firma del kernel y un subconjunto pequeño del sistema que incluye un verificador VIB de arranque seguro.

2 El verificador VIB verifica cada paquete VIB que se instala en el sistema.

En este punto, todo el sistema arranca con la raíz de confianza en los certificados que son parte del firmware UEFI.

Solución de problemas de arranque seguro UEFI

Si no se logra un arranque seguro en ningún nivel de la secuencia de arranque, se produce un error.

El mensaje de error depende del proveedor de hardware y del nivel en el que no se pudo realizar la verificación.

- Si intenta arrancar con un cargador de arranque no firmado o alterado, se produce un error durante la secuencia de arranque. El mensaje exacto depende del proveedor de hardware. Se puede parecer al siguiente error o ser diferente.

  ```
  UEFI0073: Unable to boot PXE Device...because of the Secure Boot policy
  ```

- Si se alteró el kernel, se produce un error como el siguiente.

  ```
  Fatal error: 39 (Secure Boot Failed)
  ```

- Si se alteró un paquete (VIB o controlador), se muestra una pantalla violeta con el siguiente mensaje.

  ```
  UEFI Secure Boot failed:
  Failed to verify signatures of the following vibs (XX)
  ```

Para resolver problemas con el arranque seguro, siga estos pasos.

1 Reinicie el host con el arranque seguro deshabilitado.

2 Ejecute el script de verificación de arranque seguro (consulte Ejecutar el script de validación de arranque seguro en un host ESXi actualizado).

3 Examine la información en el archivo `/var/log/esxupdate.log`.

Ejecutar el script de validación de arranque seguro en un host ESXi actualizado

Después de actualizar un host ESXi a partir de una versión anterior de ESXi que no admitía el arranque seguro UEFI, es posible que pueda habilitar el arranque seguro. La posibilidad de habilitar el arranque seguro depende de la forma en la que realizó la actualización y de si esta reemplazó todos los VIB existentes o dejó alguno sin modificar. Puede ejecutar el script de validación después de realizar la actualización para determinar si la instalación actualizada admite el arranque seguro.

Para que el arranque seguro se realice correctamente, la firma de cada VIB instalado debe estar disponible en el sistema. Las versiones anteriores de ESXi no guardan las firmas cuando se instalan los VIB.

- Si realiza la actualización mediante comandos ESXCLI, la versión anterior de ESXi instalará los nuevos VIB, por lo que no se guardarán las firmas y no será posible realizar el arranque seguro.
- Si realiza la actualización mediante el archivo ISO, se guardarán las firmas de los nuevos VIB. Esto también es así para las actualizaciones de vSphere Upgrade Manager que utilicen el archivo ISO.

- Si los VIB anteriores permanecen en el sistema, las firmas de dichos VIB no estarán disponibles y no será posible realizar el arranque seguro.
  - Si el sistema utiliza un controlador de terceros y la actualización de VMware no incluye una nueva versión del VIB de controlador, el VIB anterior permanecerá en el sistema tras la actualización.
  - En casos excepcionales, VMware puede descartar el desarrollo en curso de un VIB específico sin proporcionar un nuevo VIB que lo reemplace o lo deje obsoleto, de manera que el VIB anterior permanece en el sistema tras la actualización.

Nota El arranque seguro UEFI también requiere un cargador de arranque actualizado. Este script no comprueba que haya un cargador de arranque actualizado.

Requisitos previos

- Verifique que el hardware admita el arranque seguro UEFI.
- Verifique que todos los VIB estén firmados con un nivel de aceptación PartnerSupported, como mínimo. Si incluye VIB en el nivel CommunitySupported, no podrá usar el arranque seguro.

Procedimiento

1 Actualice ESXi y ejecute el siguiente comando.

```
/usr/lib/vmware/secureboot/bin/secureBoot.py -c
```

2 Compruebe el resultado.

El resultado incluye `Secure boot can be enabled` o `Secure boot CANNOT be enabled`.

Proteger hosts ESXi con el módulo de plataforma de confianza

Los hosts ESXi pueden utilizar los chips de los módulos de plataforma de confianza (Trusted Platform Module, TPM), los cuales son procesadores criptográficos seguros que mejoran la seguridad de los hosts, ya que proporcionan una garantía de confianza con acceso raíz en el hardware en lugar de en el software.

TPM es un estándar de la industria para los procesadores criptográficos seguros. Los chips TPM se utilizan en la mayoría de los equipos actuales, desde portátiles hasta equipos de escritorio y servidores. vSphere 6.7 y las versiones posteriores son compatibles con la versión 2.0 de TPM.

Un chip TPM 2.0 atesta la identidad de un host ESXi. La atestación de host es el proceso de autenticar y avalar el estado de software del host en un momento específico. El arranque seguro UEFI, por el cual solo se carga software firmado en el arranque, es un requisito para la atestación exitosa. El chip TPM 2.0 registra y almacena de forma segura las mediciones de los módulos de software arrancados en el sistema, lo que vCenter Server verifica de forma remota.

Los pasos de alto nivel del proceso de atestación remota son:

1 Establecer la confiabilidad del TPM remoto y crear una clave de atestación (Attestation Key, AK) en el módulo.

   Cuando un host ESXi se agrega a, se reinicia desde o se vuelve a conectar a vCenter Server, vCenter Server solicita una AK del host. Una parte del proceso de creación de AK también implica la verificación del hardware de TPM para garantizar que lo haya producido un proveedor conocido (y de confianza).

2 Recuperar el informe de atestación del host.

   vCenter Server solicita que el host envíe un informe de atestación, el cual incluye una oferta de los registros de configuración de la plataforma (Platform Configuration Registers, PCR), firmada por TPM, y otros metadatos binarios de host firmados. Al comprobar que la información corresponde a una configuración que se considera de confianza, una instancia de vCenter Server identifica la plataforma en un host que anteriormente no era de confianza.

3 Comprobar la autenticidad del host.

   vCenter Server verifica la autenticidad de la oferta firmada, deduce las versiones de software y determina la confiabilidad de las versiones de dicho software. Si vCenter Server determina que la oferta firmada no es válida, se produce un error en la atestación remota y el host no se considera de confianza.

Para utilizar un chip TPM 2.0, el entorno de vCenter Server debe cumplir estos requisitos:

- vCenter Server 6.7 o versiones posteriores
- Host ESXi 6.7 o versión posterior con un chip TPM 2.0 instalado y habilitado en UEFI
- Arranque seguro UEFI habilitado

Asegúrese de que TPM está configurado en la BIOS del host ESXi para utilizar el algoritmo de hash SHA-256 y la interfaz TIS/FIFO (First-In, First-Out), y no CRB (Command Response Buffer). Para obtener más información acerca de cómo configurar las opciones de la BIOS necesarias, consulte la documentación del proveedor.

Consulte los chips TPM 2.0 certificados por VMware en la siguiente ubicación:

https://www.vmware.com/resources/compatibility/search.php

Al arrancar un host ESXi con un chip TPM 2.0 instalado, vCenter Server supervisa el estado de atestación del host. vSphere Client muestra el estado de confianza del hardware en la pestaña **Resumen** de vCenter Server debajo de **Seguridad** con las siguientes alarmas:

- Verde: estado Normal, es decir, plena confianza.
- Rojo: no se pudo atestar.

Nota Si agrega un chip TPM 2.0 a un host ESXi que ya administra vCenter Server, primero debe desconectar el host y, a continuación, volver a conectarlo. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener más información sobre cómo desconectar y reconectar hosts.

Demostración de la característica de ESXi y Trusted Platform Module 2.0 (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_tbf3649p/uiConfId/49694343/)

Ver el estado de atestación de un host ESXi

Cuando se agrega a un host ESXi, un chip compatible con Trusted Platform Module 2.0 atesta la integridad de la plataforma. Puede ver el estado de atestación del host en vSphere Client. También puede ver el estado de la tecnología de ejecución de confianza (Trusted Execution Technology, TXT) de Intel.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Desplácese hasta un centro de datos y haga clic en la pestaña **Supervisar**.

3 Haga clic en **Seguridad**.

4 Revise el estado del host en la columna Atestación y lea el mensaje adjunto en la columna **Mensaje**.

Pasos siguientes

Si el estado de atestación es Error o Advertencia, consulte Solucionar problemas de atestación de host ESXi.

Solucionar problemas de atestación de host ESXi

Cuando se instala un dispositivo con módulo de plataforma de confianza (Trusted Platform Module, TPM) en un host ESXi, es posible que este no pase la atestación. Puede solucionar las posibles causas de este problema.

Procedimiento

1 Puede ver el estado de la alarma del host ESXi y el correspondiente mensaje de error. Consulte Ver el estado de atestación de un host ESXi.

2 Si el mensaje de error es `Arranque seguro de host deshabilitado`, debe volver a habilitar el arranque seguro para resolver el problema.

3 Si se produce un error en el estado de atestación del host, busque el siguiente mensaje en el archivo `vpxd.log` de vCenter Server:

   ```
   No hay ninguna clave de identidad en la memoria caché; se cargará de la base de datos
   ```

   Este mensaje indica que se está agregando un chip TPM 2.0 a un host de ESXi que ya administra vCenter Server. En primer lugar, debe desconectar el host y, a continuación, volver a conectarlo. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener más información sobre cómo desconectar y reconectar hosts.

Para obtener más información sobre los archivos de registro de vCenter Server, incluidas la ubicación y la rotación de registros, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/1021804.

4 Para todos los demás mensajes es de error, póngase en contacto con soporte al cliente.

Archivos de registro de ESXi

Los archivos de registro son un componente importante para la solución de problemas de ataques y la obtención de información sobre las vulneraciones. El registro en un servidor de registro centralizado y seguro puede ayudar a prevenir la adulteración de registros. El registro remoto también proporciona un registro de auditoría a largo plazo.

Para aumentar la seguridad del host, lleve a cabo las siguientes medidas:

- Configure los registros persistentes en un almacén de datos. De forma predeterminada, los registros en los hosts ESXi se almacenan en el sistema de archivos en la memoria. Por lo tanto, se pierden con cada reinicio del host y solo se almacenan 24 horas de datos de registros. Al habilitar los registros persistentes, tiene un registro dedicado de la actividad para el host.
- El registro remoto a un host central permite recopilar archivos de registro en un host central. Desde ese host, puede supervisar todos los hosts con una sola herramienta, realizar análisis agregados y buscar datos de registros. Este enfoque facilita la supervisión y revela información sobre ataques coordinados en varios hosts.
- Utilice una CLI, como vCLI o PowerCLI, o un cliente API para configurar el syslog remoto seguro en hosts de ESXi.
- Consulte la configuración de syslog para asegurarse de que el puerto y el servidor syslog sean válidos.

Consulte la documentación de *Supervisión y rendimiento de vSphere* para obtener información sobre la configuración de syslog y sobre los archivos de registro de ESXi.

Configurar Syslog en hosts ESXi

Puede utilizar vSphere Client o el comando `esxcli system syslog` de vCLI para configurar el servicio de Syslog.

Para obtener información sobre la utilización del comando `esxcli system syslog` y otros comandos de vCLI, consulte *Introducción a ESXCLI*.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, haga clic en **Configuración avanzada del sistema**.

4 Haga clic en **Editar**.

5 Filtre por **`syslog`**.

6 Para configurar el registro de manera global, seleccione el ajuste que desea cambiar e introduzca el valor.

Opción	Descripción
Syslog.global.defaultRotate	Cantidad máxima de archivos que desea guardar. Puede configurar este número en forma global y para subregistradores individuales.
Syslog.global.defaultSize	Tamaño predeterminado del registro, en KB, antes de que el sistema rote los registros. Puede configurar este número en forma global y para subregistradores individuales.
Syslog.global.LogDir	El directorio en el que se almacenan los registros. El directorio puede encontrarse en volúmenes NFS o VMFS montados. Solo el directorio `/scratch` del sistema de archivos local se mantiene en todos los reinicios. Especifique el directorio como [*nombrealmacéndatos*] *ruta_a_archivo*, donde la ruta de acceso es relativa a la raíz del volumen que respalda el almacén de datos. Por ejemplo, la ruta de acceso `[storage1] /systemlogs` se asigna a la ruta de acceso `/vmfs/volumes/storage1/systemlogs`.
Syslog.global.logDirUnique	Al seleccionar esta opción, se crea un subdirectorio con el nombre del host ESXi del directorio especificado por **Syslog.global.LogDir**. Un directorio único es útil si varios hosts ESXi utilizan el mismo directorio NFS.
Syslog.global.LogHost	El host remoto al que se reenvían los mensajes de syslog y el puerto en el que el host remoto recibe mensajes de syslog. Puede incluir el protocolo y el puerto; por ejemplo, `ssl://nombreHost1:1514`. Se admiten UDP (solo en el puerto 514), TCP y SSL. El host remoto debe tener syslog instalado y configurado correctamente para recibir los mensajes de syslog reenviados. Consulte la documentación del servicio de Syslog instalado en el host remoto para obtener información sobre la configuración.

7 (opcional) Para sobrescribir los valores predeterminados de tamaño de registro y rotación de registros de cualquier registro:

   a Haga clic en el nombre del registro que desea personalizar.

   b Introduzca el número de rotaciones y el tamaño de registro que desea.

8 Haga clic en **Aceptar**.

Resultados

Los cambios en las opciones de syslog se aplican de inmediato.

Ubicaciones de archivos de registro de ESXi

ESXi registra la actividad de los hosts en los archivos de registro, mediante una funcionalidad de Syslog.

Componente	Ubicación	Propósito
VMkernel	`/var/log/vmkernel.log`	Registra las actividades relacionadas con máquinas virtuales y ESXi.
Advertencias de VMkernel	`/var/log/vmkwarning.log`	Registra las actividades relacionadas con máquinas virtuales.
Resumen de VMkernel	`/var/log/vmksummary.log`	Se utiliza para determinar las estadísticas de disponibilidad y tiempo de actividad de ESXi (valores separados por comas).
Registro del agente del host ESXi	`/var/log/hostd.log`	Contiene información sobre el agente que administra y configura el host ESXi y sus máquinas virtuales.
Registro del agente de vCenter	`/var/log/vpxa.log`	Contiene información sobre el agente que se comunica con vCenter Server (si el host es administrado por vCenter Server).
Registro del shell	`/var/log/shell.log`	Contiene un registro de todos los comandos introducidos en ESXi Shell y también de todos los eventos del shell (por ejemplo, el momento en que se habilitó el shell).
Autenticación	`/var/log/auth.log`	Contiene todos los eventos relacionados con la autenticación para el sistema local.
Mensajes del sistema	`/var/log/syslog.log`	Contiene todos los mensajes del registro general y puede usarse para solución de problemas. Esta información antes se encontraba en los mensajes del archivo de registro.
Máquinas virtuales	El mismo directorio en el que se encuentran los archivos de configuración de la máquina virtual afectada, denominados vmware.log y vmware*.log. Por ejemplo, /vmfs/volumes/*datastore*/*virtual machine*/vwmare.log	Contiene todos los eventos relacionados con el encendido de la máquina virtual, la información de errores del sistema, la actividad y el estado de las herramientas, la sincronización de hora, los cambios en el hardware virtual, las migraciones de vMotion, los clones de la máquina, etc.
Arranque rápido	`/var/log/loadESX.log`	Contiene todos los eventos relacionados con el reinicio de un host ESXi a través del arranque rápido.

Proteger tráfico de registro de Fault Tolerance

VMware Fault Tolerance (FT) captura las entradas y los eventos que se producen en una máquina virtual principal y los envía a la máquina virtual secundaria, que se ejecuta en otro host.

Este tráfico de registro entre la máquina virtual principal y la secundaria está descifrado y contiene datos de la red invitada y de la E/S de almacenamiento, así como también contenido de memoria del sistema operativo invitado. Este tráfico puede incluir datos confidenciales, como contraseñas en texto sin formato. Para evitar que estos datos se divulguen, asegúrese de que la red esté protegida, especialmente contra ataques de intermediarios ("Man in the middle"). Por ejemplo, use una red privada para el tráfico de registro de FT.

Proteger sistemas vCenter Server

4

La protección de vCenter Server incluye la seguridad del host en el que se ejecuta vCenter Server, el cumplimiento de las prácticas recomendadas para asignar privilegios y funciones, y la comprobación de la integridad de los clientes que se conectan a vCenter Server.

Este capítulo incluye los siguientes temas:

- Prácticas recomendadas de seguridad de vCenter Server
- Comprobar huellas digitales para hosts ESXi heredados
- Puertos necesarios para vCenter Server y Platform Services Controller

Prácticas recomendadas de seguridad de vCenter Server

Seguir las prácticas recomendadas de seguridad para vCenter Server ayuda a garantizar la integridad del entorno de vSphere.

Prácticas recomendadas sobre el control de acceso a vCenter Server

Realice un control estricto del acceso a los diferentes componentes de vCenter Server a fin de aumentar la seguridad del sistema.

Las siguientes instrucciones ayudan a garantizar la seguridad del entorno.

Usar cuentas con nombre

- Si la cuenta local de administrador de Windows actualmente tiene la función de administrador de vCenter Server, elimine esa función y asígnesela a una o más cuentas de administrador con nombre de vCenter Server. Otorgue la función de administrador únicamente a aquellos administradores que la necesiten. Se pueden crear funciones personalizadas o se puede usar la función de administrador Sin criptografía para los administradores que tienen privilegios más limitados. No aplique esta función a cualquier grupo cuya pertenencia no esté estrictamente controlada.

  Nota A partir de vSphere 6.0, el administrador local ya no cuenta con derechos administrativos completos para acceder a vCenter Server de forma predeterminada.

- Instale vCenter Server mediante una cuenta de servicio en lugar de hacerlo desde una cuenta de Windows. La cuenta de servicio debe ser un administrador en la máquina local.

- Compruebe que las aplicaciones usen cuentas de servicio únicas al conectarse a un sistema vCenter Server.

Supervisar los privilegios de los usuarios administradores de vCenter Server

No todos los usuarios administradores deben tener la función de administrador. En cambio, se puede crear una función personalizado con el conjunto adecuado de privilegios y asignárselo a otros administradores.

Los usuarios con la función de administrador de vCenter Server tienen privilegios sobre todos los objetos de la jerarquía. Por ejemplo, la función de administrador permite, de forma predeterminada, que los usuarios interactúen con los archivos y los programas que se encuentran en el sistema operativo invitado de la máquina virtual. Si se asigna esa función a demasiados usuarios, se puede reducir la confidencialidad, la disponibilidad o la integridad de los datos de la máquina virtual. Cree una función que les otorgue a los administradores los privilegios que necesitan, pero elimine algunos de los privilegios de administración de la máquina virtual.

Minimizar el acceso

No permita que los usuarios inicien sesión directamente en el equipo host de vCenter Server. Los usuarios que inician sesión en el equipo host de vCenter Server pueden llegar a causar daños, ya sea intencionales o involuntarios, al alterar la configuración y modificar los procesos. Esos usuarios pueden llegar a acceder a las credenciales de vCenter, como el certificado SSL. Permita iniciar sesión en el sistema solo a los usuarios que puedan realizar tareas legítimas y asegúrese de que se auditen los eventos de inicio de sesión.

Otorgar privilegios mínimos a los usuarios de bases de datos de vCenter Server

El usuario de base de datos precisa solamente ciertos privilegios específicos para el acceso a la base de datos.

Algunos privilegios son necesarios solamente para la instalación y las actualizaciones. Estos privilegios se pueden eliminar desde el administrador de la base de datos una vez que vCenter Server se haya instalado o actualizado.

Restringir el acceso al explorador del almacén de datos

Asigne el privilegio **Almacén de datos.Examinar almacén de datos** solo a los usuarios o grupos que realmente lo necesitan. Los usuarios que tienen el privilegio pueden ver, cargar o descargar archivos en almacenes de datos asociados con la implementación de vSphere a través del explorador web o vSphere Client

Restringir a los usuarios la ejecución de comandos en una máquina virtual

De forma predeterminada, un usuario con la función de administrador de vCenter Server puede interactuar con archivos y programas en el sistema operativo invitado de una máquina virtual. Para reducir el riesgo de infracciones de confidencialidad, disponibilidad o integridad del invitado, cree una función personalizada de acceso que no sea de invitado sin el privilegio **Operaciones de invitado**. Consulte Restringir la ejecución de comandos dentro de una máquina virtual a los usuarios.

Considerar la modificación de la directiva de contraseñas para vpxuser

De manera predeterminada, vCenter Server cambia la contraseña de vpxuser automáticamente cada 30 días. Asegúrese de que esta configuración respete la directiva de la empresa o configure la directiva de contraseñas de vCenter Server. Consulte Configurar la directiva de contraseñas de vCenter Server.

Nota Compruebe que la directiva de caducidad de contraseñas no sea demasiado corta.

Comprobar los privilegios después de reiniciar vCenter Server

Revise la reasignación de privilegios al reiniciar vCenter Server. Si el usuario o el grupo que tienen la función de administrador en la carpeta raíz no se pueden validar durante el reinicio, la función se elimina de ese usuario o grupo. En su lugar, vCenter Server otorga la función de administrador al administrador de vCenter Single Sign-On, administrator@vsphere.local de forma predeterminada. De ese modo, esta cuenta puede actuar como administrador de vCenter Server.

Restablezca la cuenta de administrador con nombre y asigne la función de administrador a dicha cuenta para evitar usar la cuenta de administrador anónima de vCenter Single Sign-On (de manera predeterminada, administrator@vsphere.local).

Usar niveles altos de cifrado RDP

Asegúrese de que en cada equipo con Windows de la infraestructura se establezca una configuración del host mediante Remote Desktop a fin de garantizar el nivel más alto de cifrado adecuado para el entorno.

Comprobar certificados de vSphere Client

Indique a los usuarios de vSphere Client o de otras aplicaciones cliente que pongan atención a las advertencias de comprobación de certificados. Sin la comprobación de certificados, el usuario puede ser víctima de un ataque de MiTM.

Configurar la directiva de contraseñas de vCenter Server

De manera predeterminada, vCenter Server cambia la contraseña de vpxuser automáticamente cada 30 días. Puede cambiar este valor desde vSphere Client.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Client.

2 Seleccione el sistema de vCenter Server en la jerarquía de objetos.

3 Haga clic en **Configurar**.

4 Haga clic en **Configuración avanzada** y en **Editar configuración**.

5 Haga clic en el icono **Filtrar** e introduzca **`VimPasswordExpirationInDays`**.

6 Configure `VirtualCenter.VimPasswordExpirationInDays` para que cumpla con sus requisitos.

Quitar certificados caducados o revocados, y registros de instalaciones con errores

Dejar certificados caducados o revocados, o dejar registros de instalación incorrecta de vCenter Server en el sistema vCenter Server puede perjudicar el entorno.

Los certificados caducados o revocados deben eliminarse por los siguientes motivos.

- Si los certificados caducados o revocados no se eliminan del sistema vCenter Server, el entorno puede quedar vulnerable a un ataque de MiTM.
- En ciertos casos, si la instalación de vCenter Server no se realiza correctamente, se crea en el sistema un archivo de registro que contiene la contraseña de la base de datos en texto sin formato. Un atacante que logre entrar al sistema vCenter Server puede tener acceso a esta contraseña y, al mismo tiempo, acceder a la base de datos de vCenter Server.

Proteger el host de Windows para vCenter Server

Para proteger el host de Windows donde se ejecuta vCenter Server contra vulnerabilidades y ataques, garantice que el entorno del host sea lo más seguro posible.

- Mantenga un sistema operativo, una base de datos y hardware compatibles para el sistema vCenter Server. Si vCenter Server no se ejecuta en un sistema operativo compatible, es posible que no funcione correctamente, y vCenter Server queda vulnerable a posibles ataques.
- Mantenga el sistema vCenter Server actualizado con las revisiones adecuadas. Cuando el servidor está actualizado con las revisiones del sistema operativo, es menos vulnerable a posibles ataques.
- Proteja al sistema operativo en el host de vCenter Server. La protección incluye software antivirus y antimalware.
- Asegúrese de que en cada equipo con Windows de la infraestructura se establezca una configuración del host mediante Remote Desktop (RDP) a fin de garantizar el nivel más alto de cifrado, conforme a las directrices estándar de la industria o a las instrucciones internas.

Para obtener información sobre la compatibilidad del sistema operativo y la base de datos, consulte *Matrices de compatibilidad de vSphere*.

Limitar la conectividad de red de vCenter Server

Para mejorar la seguridad, evite colocar el sistema vCenter Server en otra red distinta de la red de administración, y asegúrese de que el tráfico de administración de vSphere se encuentre en una red restringida. Al limitar la conectividad de red, se limitan ciertos tipos de ataques.

vCenter Server requiere acceso solamente a una red de administración. Evite colocar el sistema vCenter Server en otras redes, como la red de producción o la de almacenamiento, o en otra red con acceso a Internet. vCenter Server no necesita acceder a la red donde funciona vMotion.

vCenter Server requiere conectividad de red con los siguientes sistemas.

- Todos los hosts ESXi.
- La base de datos de vCenter Server.
- Otros sistemas de vCenter Server (si los sistemas de vCenter Server forman parte de un dominio de vCenter Single Sign-On común con fines de replicación de etiquetas, permisos, etc.).
- Los sistemas que están autorizados para ejecutar clientes de administración. Por ejemplo, vSphere Client, un sistema Windows donde se utiliza PowerCLI o cualquier otro cliente basado en SDK.
- Los sistemas que ejecutan componentes complementarios como VMware vSphere Update Manager.
- Los servicios de infraestructura como DNS, Active Directory y NTP.
- Otros sistemas que ejecutan componentes fundamentales para la funcionalidad del sistema vCenter Server.

Utilice un firewall local en el sistema Windows donde el sistema vCenter Server se está ejecutando o utilice un firewall de red. Incluya restricciones de acceso basadas en IP de modo que solo los componentes necesarios puedan comunicarse con el sistema vCenter Server.

Evaluación del uso de clientes Linux con CLI y SDK

Las comunicaciones entre los componentes del cliente y el sistema vCenter Server o los hosts ESXi están protegidas por un cifrado basado en SSL de forma predeterminada. Las versiones de Linux de estos componentes no realizan la validación de certificados. Considere restringir el uso de estos clientes.

Para mejorar la seguridad, puede reemplazar los certificados firmados por VMCA del sistema de vCenter Server y los hosts ESXi por certificados firmados por una entidad de certificación de la empresa o de terceros. Sin embargo, ciertas comunicaciones con clientes Linux seguirán siendo vulnerables a ataques man-in-the-middle. Los siguientes componentes son vulnerables cuando se ejecutan en el sistema operativo Linux.

- Comandos de vCLI
- Scripts de vSphere SDK for Perl
- Programas escritos con el vSphere Web Services SDK

Si aplica los controles correspondientes, puede reducir la restricción contra el uso de clientes Linux.

- Restrinja el acceso a la red de administración únicamente a los sistemas autorizados.
- Utilice firewalls para garantizar que únicamente los hosts autorizados tengan permiso para acceder a vCenter Server.
- Utilice sistemas JumpBox para garantizar que los clientes Linux sean supervisados.

Examinar los complementos del cliente

Las extensiones de vSphere Client y vSphere Web Client se ejecutan en el mismo nivel de privilegio que el usuario que inició sesión. Una extensión maliciosa puede enmascararse como un complemento útil y realizar operaciones dañinas, como el robo de credenciales o cambios en la configuración del sistema. Para aumentar la seguridad, utilice una instalación en la que se incluyan únicamente extensiones autorizadas de orígenes confiables.

Una instalación de vCenter incluye un marco de extensibilidad para vSphere Client y vSphere Web Client. Este marco se puede usar para extender los clientes con selecciones de menú o iconos de la barra de herramientas. Las extensiones pueden proporcionar acceso a los componentes de complementos de vCenter o la funcionalidad externa basada en web.

Al utilizar el marco de extensibilidad, se entraña el riesgo de introducir funcionalidades no intencionadas. Por ejemplo, si un administrador instala un complemento en una instancia de vSphere Client, el complemento puede ejecutar comandos arbitrarios con el nivel de privilegio de ese administrador.

Para evitar una posible transigencia de vSphere Client o vSphere Web Client, examine periódicamente todos los complementos instalados y compruebe que cada uno provenga de un origen de confianza.

Requisitos previos

Debe tener los privilegios necesarios para acceder al servicio vCenter Single Sign-On. Estos privilegios difieren de los de vCenter Server.

Procedimiento

1. Inicie sesión en el cliente como administrator@vsphere.local o como usuario con privilegios de vCenter Single Sign-On.
2. En la página de inicio, seleccione **Administración** y, a continuación, seleccione **Complementos del cliente** en **Soluciones**.
3. Examine la lista de complementos del cliente.

Prácticas recomendadas de seguridad de vCenter Server Appliance

Siga todas las prácticas recomendadas de seguridad del sistema vCenter Server para proteger vCenter Server Appliance. Se proporcionan pasos adicionales a modo de ayuda para aumentar la seguridad del dispositivo.

Configure NTP

Asegúrese de que todos los sistemas utilicen el mismo origen de hora relativo. Este origen de hora debe estar sincronizado con un estándar de hora acordado, como la hora universal coordinada (Coordinated Universal Time, UTC). Es fundamental que los sistemas estén sincronizados para la validación de certificados. NTP también facilita el rastreo de intrusos en los archivos de registro. Una configuración de hora incorrecta dificulta la inspección y la correlación de los archivos de registro para detectar ataques, además de hacer imprecisas las auditorías. Consulte Sincronizar la hora de vCenter Server Appliance con un servidor NTP.

Restrinja el acceso a la red de vCenter Server Appliance.

Restrinja el acceso a los componentes que se necesiten para comunicarse con vCenter Server Appliance. Al bloquear el acceso desde sistemas innecesarios, se reducen las posibilidades de que el sistema operativo reciba ataques.

Para obtener la lista de todos los puertos y protocolos compatibles en los productos de VMware, incluidos vSphere y vSAN, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/. Puede buscar puertos por producto de VMware, crear una lista de puertos personalizada e imprimir o guardar listas de puertos.

Configurar un host bastión

Para ayudar a proteger los activos, configure un host bastión (también denominado Jump Box) para realizar tareas administrativas con privilegios elevados. Un host bastión es un equipo con un propósito especial que aloja una cantidad mínima de aplicaciones administrativas. Se eliminan todos los demás servicios innecesarios. El host suele residir en la red de administración. Un host bastión aumenta la protección de los activos mediante la restricción del inicio de sesión a los individuos clave, la solicitud de reglas de firewall para iniciar sesión y la adición de supervisión mediante herramientas de auditoría.

Requisitos de contraseñas y comportamiento de bloqueo de vCenter

Para administrar el entorno de vSphere, debe conocer la directiva de contraseñas de vCenter Single Sign-On, de las contraseñas de vCenter Server y el comportamiento de bloqueo.

En esta sección se analizan las contraseñas de vCenter Single Sign-On. Consulte Bloqueo de cuenta y contraseñas ESXi, donde se analizan las contraseñas de los usuarios locales de ESXi.

Contraseña para el administrador de vCenter Single Sign-On

La contraseña predeterminada del administrador de vCenter Single Sign-On, administrator@vsphere.local, se especifica en la directiva de contraseñas de vCenter Single Sign-On. De manera predeterminada, esta contraseña debe cumplir con los siguientes requisitos:

- Tener al menos ocho caracteres
- Tener al menos un carácter en minúscula
- Tener al menos un carácter numérico
- Tener al menos un carácter especial

La contraseña de este usuario no puede superar los 20 caracteres. A partir de vSphere 6.0, se permitirán caracteres que no son ASCII. Los administradores pueden cambiar la directiva de contraseñas predeterminada. Consulte la documentación de *Administrar Platform Services Controller*.

Contraseñas de vCenter Server

En vCenter Server, los requisitos de contraseñas se determinan mediante vCenter Single Sign-On o por el origen de identidad configurada, que puede ser Active Directory, OpenLDAP.

Comportamiento de bloqueo de vCenter Single Sign-On

Los usuarios quedan bloqueados después de una cantidad preestablecida de intentos consecutivos con errores. De manera predeterminada, los usuarios quedan bloqueados después de cinco intentos consecutivos fallidos en tres minutos, y una cuenta bloqueada se desbloquea automáticamente transcurridos cinco minutos. Se pueden cambiar estos valores predeterminados a través de la directiva de bloqueo de vCenter Single Sign-On. Consulte la documentación de *Administrar Platform Services Controller*.

A partir de vSphere 6.0, el administrador de dominio predeterminado de vCenter Single Sign-On, administrator@vsphere.local, no se verá afectado por la directiva de bloqueo. El usuario se ve afectado por la directiva de contraseñas.

Cambios de contraseña

Si conoce su contraseña, puede cambiarla mediante el comando `dir-cli password change`. Si olvida su contraseña, un administrador de vCenter Single Sign-On puede restablecerla con el comando `dir-cli password reset`.

Busque información acerca de la caducidad de la contraseña y temas relacionados de diversas versiones de vSphere en la base de conocimientos de VMware.

Comprobar huellas digitales para hosts ESXi heredados

En vSphere 6 y las versiones posteriores, se asignan certificados de VMCA a los hosts de forma predeterminada. Si cambia el modo de certificación a Huella digital, puede continuar usando este modo para los hosts heredados. Puede comprobar las huellas digitales en vSphere Client.

Nota De manera predeterminada, los certificados se conservan en todas las actualizaciones.

Procedimiento

1 Desplácese hasta vCenter Server en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En **Configuración**, haga clic en **General**.

4 Haga clic en **Editar**.

5 Haga clic en **Configuración de SSL**.

6 Si alguno de los hosts ESXi 5.5 o de versiones anteriores necesita una validación manual, compare las huellas digitales detalladas para los hosts con las huellas digitales de la consola del host.

   Para obtener la huella digital del host, use la interfaz de usuario de la consola directa (DCUI).

   a Inicie sesión en la consola directa y presione F2 para acceder al menú Personalización del sistema.

   b Seleccione **Ver información de soporte**.

      La huella digital del host se muestra en la columna a la derecha.

7 Si la huella digital coincide, active la casilla **Comprobar** ubicada junto al host.

   Los hosts no seleccionados se desconectan después de hacer clic en **Aceptar**.

8 Haga clic en **Guardar**.

Puertos necesarios para vCenter Server y Platform Services Controller

El sistema vCenter Server, tanto en Windows como en el dispositivo, debe poder enviar datos a cada host administrado y recibir datos de los servicios de vSphere Client y Platform Services Controller. Para permitir las actividades de migración y aprovisionamiento entre los hosts administrados, los hosts de origen y de destino deben poder recibir datos de cada uno.

Se puede acceder a vCenter Server a través de los puertos TCP y UDP predeterminados. Si administra componentes de red desde afuera de un firewall, es posible que se le pida que vuelva a configurar el firewall para permitir el acceso en los puertos necesarios. Para obtener la lista de todos los puertos y protocolos compatibles en vCenter Server, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/.

Durante la instalación, si un puerto se encuentra en uso o está bloqueado mediante una lista de no permitidos, el instalador de vCenter Server mostrará un mensaje de error. Debe utilizar otro número de puerto para continuar con la instalación.

VMware utiliza los puertos designados para la comunicación. Asimismo, los hosts administrados supervisan los puertos designados para los datos desde vCenter Server. Si existe un firewall integrado entre cualquiera de estos elementos, el instalador abre los puertos durante el proceso de instalación o actualización. En el caso de firewalls personalizados, debe abrir manualmente los puertos requeridos. Si posee un firewall entre dos hosts administrados y desea realizar actividades en el origen o destino, como la migración o clonación, debe configurar un medio para que los hosts administrados puedan recibir datos.

Para configurar el sistema vCenter Server a fin de que utilice un puerto diferente donde recibir los datos de vSphere Client, consulte la documentación de *Administrar vCenter Server y hosts*.

Proteger máquinas virtuales

5

El sistema operativo invitado que se ejecuta en la máquina virtual está sujeto a los mismos riesgos de seguridad que un sistema físico. Proteja las máquinas virtuales como se protegen las máquinas físicas. Siga las prácticas recomendadas que se describen en este documento y en la *guía de configuración de seguridad* (anteriormente denominada la *Guía de fortalecimiento*).

La *guía de configuración de seguridad* está disponible en https://core.vmware.com/security.

Este capítulo incluye los siguientes temas:

- Habilitar o deshabilitar el arranque seguro UEFI para una máquina virtual
- Limitación de los mensajes informativos de máquinas virtuales a archivos VMX
- Prácticas recomendadas de seguridad para las máquinas virtuales

Habilitar o deshabilitar el arranque seguro UEFI para una máquina virtual

El arranque seguro UEFI es un estándar de seguridad que permite garantizar que el equipo arranque usando solamente software de confianza para el fabricante del equipo. Para ciertos sistemas operativos y versiones de hardware de máquinas virtuales, se puede habilitar el arranque seguro del mismo modo que para una máquina física.

En un sistema operativo que admite el arranque seguro UEFI, cada parte del software de arranque está firmada, incluidos el cargador de arranque, el kernel del sistema operativo y los controladores del sistema operativo. La configuración predeterminada de la máquina virtual incluye varios certificados de firma de código.

- Un certificado de Microsoft que se utiliza solamente para el arranque de Windows.
- Un certificado de Microsoft que se utiliza para código de terceros firmado por Microsoft, como los cargadores de arranque de Linux.
- Un certificado de VMware que solo se utiliza para el arranque de ESXi dentro de una máquina virtual.

La configuración predeterminada de la máquina virtual incluye un certificado para que las solicitudes de autenticación modifiquen la configuración de arranque seguro, incluida la lista de revocación de arranque seguro, desde el interior de la máquina virtual. Se trata de un certificado de clave de intercambio de claves (Key Exchange Key, KEK) de Microsoft.

En casi todos los casos, no es necesario reemplazar los certificados existentes. Si no desea reemplazar los certificados, consulte la base de conocimientos de VMware.

Se requiere la versión 10.1 o posterior de VMware Tools para las máquinas virtuales que utilizan el arranque seguro UEFI. Puede actualizar esas máquinas virtuales a una versión posterior de VMware Tools cuando esté disponible.

Para las máquinas virtuales Linux, no se admite VMware Host-Guest Filesystem en el modo de arranque seguro. Quite VMware Host-Guest Filesystem de VMware Tools antes de habilitar el arranque seguro.

Nota Si activa el arranque seguro de una máquina virtual, solo puede cargar controladores firmados en ella.

En esta tarea, se describe cómo usar vSphere Client para habilitar y deshabilitar el arranque seguro de una máquina virtual. También puede escribir scripts para administrar la configuración de la máquina virtual. Por ejemplo, puede automatizar el cambio del firmware de BIOS a EFI para máquinas virtuales con el siguiente código de PowerCLI:

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

Para obtener más información, consulte la *Guía del usuario de VMware PowerCLI*.

Requisitos previos

Puede habilitar el arranque seguro solamente si se cumplen los requisitos previos. Si no se cumplen, la casilla no estará visible en vSphere Client.

- Compruebe que el sistema operativo y el firmware de la máquina virtual admitan el arranque UEFI.
  - Firmware EFI.
  - Versión de hardware virtual 13 o posterior.
  - Sistema operativo que admita el arranque seguro UEFI.

  Nota Algunos sistemas operativos invitados no permiten cambiar el arranque del BIOS por el arranque UEFI sin realizar modificaciones al sistema operativo invitado. Consulte la documentación del sistema operativo invitado antes de cambiar al arranque UEFI. Si se actualiza una máquina virtual que ya utiliza el arranque UEFI a un sistema operativo que admite el arranque seguro UEFI, se puede habilitar el arranque seguro de esa máquina virtual.

- Apague la máquina virtual. Si la máquina virtual está en ejecución, la casilla aparece atenuada.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

3 Haga clic en la pestaña **Opciones de máquina virtual** y expanda **Opciones de arranque**.

4 En **Opciones de arranque**, asegúrese de que el firmware esté establecido en **EFI**.

5 Seleccione la tarea en cuestión.

   - Seleccione la casilla **Arranque seguro** para habilitar el arranque seguro.
   - Anule la selección de la casilla **Arranque seguro** para deshabilitar el arranque seguro.

6 Haga clic en **Aceptar**.

Resultados

Cuando la máquina virtual arranca, solo se permiten los componentes con firmas válidas. El proceso de arranque se detiene y muestra un error si detecta que existe un componente al que le falta una firma o cuya firma no es válida.

Limitación de los mensajes informativos de máquinas virtuales a archivos VMX

Limite los mensajes informativos de la máquina virtual al archivo VMX para evitar llenar el almacén de datos y provocar la denegación de servicio (DoS). La denegación de servicio se produce cuando no se controla el tamaño del archivo VMX de una máquina virtual y la cantidad de información supera la capacidad del almacén de datos.

De manera predeterminada, el límite del archivo de configuración de la máquina virtual (archivo VMX) es de 1 MB. En general, esta capacidad es suficiente, pero puede cambiar este valor si es necesario. Por ejemplo, puede aumentar el límite si almacena grandes cantidades de información personalizada en el archivo.

Nota Determine cuidadosamente la cantidad de información que necesita. Si la cantidad de información supera la capacidad del almacén de datos, se puede producir una denegación de servicio.

El límite predeterminado de 1 MB se aplica incluso cuando el parámetro `tools.setInfo.sizeLimit` no figura en la lista de opciones avanzadas.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Seleccione **Opciones de máquina virtual**.

4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.

5 Agregue o edite el parámetro `tools.setInfo.sizeLimit`.

Prácticas recomendadas de seguridad para las máquinas virtuales

Seguir las prácticas recomendadas de seguridad para las máquinas virtuales ayuda a garantizar la integridad de la implementación de vSphere.

- Protección general de la máquina virtual

  La máquina virtual es, en muchos aspectos, el equivalente a un servidor físico. Implemente las mismas medidas de seguridad en las máquinas virtuales que las que implementa en los sistemas físicos.

- Usar plantillas para implementar máquinas virtuales

  Cuando instala manualmente sistemas operativos invitados y aplicaciones en una máquina virtual, se introduce el riesgo de una configuración incorrecta. Mediante el uso de una plantilla que captura la imagen del sistema operativo base, protegido, sin aplicaciones instaladas, es posible garantizar que todas las máquinas virtuales se creen con un nivel de línea base conocido de seguridad.

- Minimizar el uso de la consola de la máquina virtual

  La consola de máquina virtual cumple la misma función en la máquina virtual que el monitor de un servidor físico. Los usuarios que tienen acceso a la consola de la máquina virtual tienen acceso a la administración de energía de la máquina virtual y a los controles de conectividad del dispositivo extraíble. Por lo tanto, el acceso a la consola puede permitir que ocurra un ataque malicioso en una máquina virtual.

- Evitar que las máquinas virtuales asuman el control de los recursos

  Cuando una máquina virtual consume tantos recursos del host que las demás máquinas virtuales presentes en el host no pueden realizar sus respectivas funciones, es posible que se produzca una denegación de servicio (DoS). Para evitar que una máquina virtual provoque una DoS, use las características de administración de recursos del host, como los recursos compartidos de configuración y los grupos de recursos.

- Deshabilitar funciones innecesarias en máquinas virtuales

  Cualquier servicio que se esté ejecutando en una máquina virtual conlleva un potencial ataque. Al deshabilitar los componentes del sistema que no son necesarios para admitir la aplicación o el servicio que está en ejecución en el sistema, se reduce el potencial.

Protección general de la máquina virtual

La máquina virtual es, en muchos aspectos, el equivalente a un servidor físico. Implemente las mismas medidas de seguridad en las máquinas virtuales que las que implementa en los sistemas físicos.

Siga estas prácticas recomendadas para proteger la máquina virtual:

Revisiones y otros tipos de protección

Mantenga todas las medidas de seguridad actualizadas, incluidas las revisiones adecuadas. Es fundamental realizar un seguimiento de las actualizaciones para las máquinas virtuales inactivas que están apagadas, ya que podrían pasarse por alto. Por ejemplo, asegúrese de que el software antivirus, el software antispyware, la detección de intrusos y otros tipos de protección estén habilitados para cada máquina virtual de la infraestructura virtual. También debe asegurarse de que tiene suficiente espacio para los registros de las máquinas virtuales.

Análisis antivirus

Debido a que las máquinas virtuales alojan un sistema operativo estándar, se deben proteger contra virus con un software antivirus. Según cómo utilice la máquina virtual, es posible que también sea necesario instalar un firewall de software.

Escalone la programación de análisis de virus, particularmente en las implementaciones que tengan gran cantidad de máquinas virtuales. El rendimiento de los sistemas en el entorno disminuye notablemente si examina todas las máquinas virtuales a la vez. Como los firewalls de software y los software antivirus pueden tener un gran consumo de la capacidad de virtualización, equilibre el uso de estas dos medidas de seguridad según el rendimiento de las máquinas virtuales, en especial si sabe que las máquinas virtuales están en un entorno de plena confianza.

Puertos serie

Los puertos serie son interfaces para conectar periféricos con la máquina virtual. Se utilizan a menudo en sistemas físicos para proporcionar una conexión directa y de bajo nivel con la consola de un servidor. El puerto serie virtual permite el mismo acceso a una máquina virtual. Los puertos serie permiten el acceso de bajo nivel, que por lo general no tiene un control estricto como el registro o los privilegios.

Usar plantillas para implementar máquinas virtuales

Cuando instala manualmente sistemas operativos invitados y aplicaciones en una máquina virtual, se introduce el riesgo de una configuración incorrecta. Mediante el uso de una plantilla que captura la imagen del sistema operativo base, protegido, sin aplicaciones instaladas, es posible garantizar que todas las máquinas virtuales se creen con un nivel de línea base conocido de seguridad.

Puede utilizar plantillas que contengan un sistema operativo protegido, revisado y adecuadamente configurado para crear otras plantillas específicas de la aplicación, o bien puede utilizar la plantilla de la aplicación para implementar máquinas virtuales.

Procedimiento

- Proporcione plantillas para la creación de máquinas virtuales que contengan implementaciones de sistemas operativos protegidos, revisados y adecuadamente configurados.

  De ser posible, también implemente aplicaciones en las plantillas. Asegúrese de que las aplicaciones no dependan de la información específica de la máquina virtual para poder implementarlas.

Pasos siguientes

Para obtener más información sobre las plantillas, consulte la documentación de *Administrar máquinas virtuales de vSphere*.

Minimizar el uso de la consola de la máquina virtual

La consola de máquina virtual cumple la misma función en la máquina virtual que el monitor de un servidor físico. Los usuarios que tienen acceso a la consola de la máquina virtual tienen acceso a la administración de energía de la máquina virtual y a los controles de conectividad del dispositivo extraíble. Por lo tanto, el acceso a la consola puede permitir que ocurra un ataque malicioso en una máquina virtual.

Procedimiento

1. Utilice servicios nativos de administración remota, como servicios de terminal y SSH, para interactuar con las máquinas virtuales.

   Otorgue acceso a la consola de máquina virtual solo cuando sea necesario.

2. Limite las conexiones a la consola de máquina virtual.

   Por ejemplo, en un entorno muy seguro, limítela a una conexión. En algunos entornos, se puede incrementar el límite si se necesitan varias conexiones simultáneas para realizar las tareas normales.

   a. En vSphere Client, apague la máquina virtual.

   b. Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

   c. Haga clic en la pestaña **Opciones de máquina virtual** y amplíe **Opciones de VMware Remote Console**.

   d. Introduzca la cantidad máxima de sesiones (por ejemplo, **2**).

   e. Haga clic en **Aceptar**.

Evitar que las máquinas virtuales asuman el control de los recursos

Cuando una máquina virtual consume tantos recursos del host que las demás máquinas virtuales presentes en el host no pueden realizar sus respectivas funciones, es posible que se produzca una denegación de servicio (DoS). Para evitar que una máquina virtual provoque una DoS, use

las características de administración de recursos del host, como los recursos compartidos de configuración y los grupos de recursos.

De forma predeterminada, todas las máquinas virtuales de un host ESXi comparten los recursos de forma equitativa. Puede utilizar los recursos compartidos y los grupos de recursos para evitar un ataque por denegación de servicio que haga que una máquina virtual consuma tantos recursos del host que las demás máquinas virtuales del mismo host no puedan realizar sus respectivas funciones.

No establezca límites ni utilice grupos de recursos hasta que comprenda completamente el impacto.

Procedimiento

1 Aprovisione cada máquina virtual solo con los recursos (CPU y memoria) suficientes para que funcione de forma adecuada.

2 Utilice los recursos compartidos para garantizar que las máquinas virtuales fundamentales tengan los recursos necesarios.

3 Agrupe las máquinas virtuales con requisitos similares en grupos de recursos.

4 En cada grupo de recursos, deje la opción de recursos compartidos con los valores predeterminados para que cada máquina virtual del grupo tenga aproximadamente la misma prioridad de recursos.

   Con esta configuración, una máquina virtual individual no puede usar más recursos que las demás máquinas virtuales del grupo de recursos.

Pasos siguientes

Consulte la documentación de *Administrar recursos de vSphere* para obtener información sobre recursos compartidos y límites.

Deshabilitar funciones innecesarias en máquinas virtuales

Cualquier servicio que se esté ejecutando en una máquina virtual conlleva un potencial ataque. Al deshabilitar los componentes del sistema que no son necesarios para admitir la aplicación o el servicio que está en ejecución en el sistema, se reduce el potencial.

Las máquinas virtuales no suelen precisar tantos servicios o tantas funciones como los servidores físicos. A la hora de virtualizar un sistema, evalúe si es necesario ese servicio o esa función en particular.

Nota Cuando sea posible, instale sistemas operativos invitados mediante los modos de instalación "mínimo" o "básico" para reducir el tamaño, la complejidad y la superficie de ataque del sistema operativo invitado.

Procedimiento

- Deshabilite los servicios que no se utilizan en el sistema operativo.

  Por ejemplo, si el sistema ejecuta un servidor de archivos, desconecte los servicios web.

- Desconecte los dispositivos físicos que no se utilizan, como unidades de CD/DVD, unidades de disquete y adaptadores USB.
- Deshabilite las funcionalidades sin utilizar, como las funciones de visualización que no se utilizan (o Carpetas compartidas de VMware), las cuales permiten el uso compartido de archivos de host con la máquina virtual (sistema de archivos invitado del host).
- Apague los protectores de pantalla.
- No ejecute el sistema X Window en los sistemas operativos invitados Linux, BSD o Solaris a menos que sea necesario.

Quitar dispositivos de hardware innecesarios

Todo dispositivo habilitado o conectado constituye un canal de ataque potencial. Los usuarios y los procesos con privilegios sobre una máquina virtual pueden conectar o desconectar dispositivos de hardware, como adaptadores de red o unidades de CD-ROM. Los atacantes pueden usar esta funcionalidad para infringir la seguridad de la máquina virtual. La eliminación de los dispositivos de hardware innecesarios permite evitar ataques.

Un atacante con acceso a una máquina virtual puede conectar o desconectar un dispositivo de hardware y acceder a información confidencial en un soporte físico que quede en un dispositivo de hardware. El atacante puede llegar a desconectar un adaptador de red para aislar la máquina virtual de su red, mediante lo cual se puede producir una denegación de servicio.

- No conecte dispositivos no autorizados a la máquina virtual.
- Elimine los dispositivos de hardware que no necesite o que no esté usando.
- Deshabilite los dispositivos virtuales innecesarios desde una máquina virtual.
- Asegúrese de que solo los dispositivos necesarios estén conectados a una máquina virtual. Rara vez las máquinas virtuales utilizan puertos serie o paralelos. Como regla general, las unidades de CD/DVD solo se conectan temporalmente durante la instalación del software.

Procedimiento

1. Desplácese hasta la máquina virtual en el inventario de vSphere Client.
2. Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.
3. Deshabilite los dispositivos de hardware que no sean necesarios.

   Compruebe también los siguientes dispositivos:

   - Unidades de disquete
   - Puertos serie

- Puertos paralelos
- controladoras USB
- unidades de CD-ROM

Deshabilitar las características de visualización que no se utilizan

Los atacantes pueden aprovechar una característica de visualización que no se utiliza para introducir un código malicioso en el entorno. Deshabilite las características que no se estén utilizando en el entorno.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Seleccione **Opciones de máquina virtual**.

4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.

5 Si corresponde, agregue o edite los siguientes parámetros.

Opción	Descripción
svga.vgaonly	Si establece este parámetro en el valor TRUE, las funciones avanzadas de gráficos dejarán de funcionar. Solo estará disponible el modo de consola de celda con caracteres. Si utiliza esta configuración, `mks.enable3d` no tendrá efecto. **Nota** Aplique esta configuración únicamente a las máquinas virtuales que no necesitan una tarjeta de video virtualizada.
mks.enable3d	Establezca este parámetro en el valor FALSE en las máquinas virtuales que no necesitan la funcionalidad 3D.

Deshabilitar características no expuestas

Las máquinas virtuales de VMware pueden funcionar tanto en un entorno de vSphere como en plataformas de virtualización alojadas, como VMware Workstation y VMware Fusion. Algunos parámetros de la máquina virtual no necesitan estar habilitados al ejecutar una máquina virtual en un entorno de vSphere. Deshabilite estos parámetros para reducir las vulnerabilidades posibles.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Seleccione **Opciones de máquina virtual**.

4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.

5 Agregue o edite los siguientes parámetros para establecerlos en el valor TRUE.

   - `isolation.tools.unity.push.update.disable`
   - `isolation.tools.ghi.launchmenu.change`
   - `isolation.tools.memSchedFakeSampleStats.disable`
   - `isolation.tools.getCreds.disable`
   - `isolation.tools.ghi.autologon.disable`
   - `isolation.bios.bbs.disable`
   - `isolation.tools.hgfsServerSet.disable`

6 Haga clic en **Aceptar**.

Impedir que Carpetas compartidas de VMware comparta archivos de host con la máquina virtual

En entornos de alta seguridad, es posible deshabilitar ciertos componentes para minimizar el riesgo de que un atacante utilice el sistema de archivos invitado del host (Host Guest File System, HGFS) para transferir archivos dentro del sistema operativo invitado.

La modificación de los parámetros descritos en esta sección solo afecta a la función Carpetas compartidas, no al servidor de HGFS que se ejecuta como parte de las herramientas de las máquinas virtuales invitadas. Adicionalmente, estos parámetros no afectan a los comandos de actualización automática y VIX que utilizan las transferencias de archivos de las herramientas.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Seleccione **Opciones de máquina virtual**.

4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.

5 Compruebe que el parámetro `isolation.tools.hgfsServerSet.disable` esté establecido en TRUE.

   Si se establece como TRUE, se evita que el proceso de VMX reciba notificaciones de los procesos de servicio, daemon o actualizador de cada herramientas acerca de la capacidad del servidor HGFS.

6 (opcional) Compruebe que el parámetro `isolation.tools.hgfs.disable` esté establecido en TRUE.

   Si se establece como TRUE, se deshabilita la función Carpetas compartidas de VMware que no se utiliza para compartir archivos de host con la máquina virtual.

Deshabilitar las operaciones para copiar y pegar entre el sistema operativo invitado y la consola remota

Las operaciones para copiar y pegar entre el sistema operativo invitado y la consola remota están deshabilitadas de forma predeterminada. Para lograr un entorno seguro, conserve la configuración predeterminada. Si necesita utilizar las operaciones para copiar y pegar, debe habilitarlas por medio de vSphere Client.

Los valores predeterminados de estas opciones se establecen para garantizar un entorno seguro. Sin embargo, debe establecerlas en True de forma explícita si desea habilitar herramientas de auditoría para comprobar si la configuración es correcta.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Seleccione **Opciones de máquina virtual**.

4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.

5 Asegúrese de que se detallen los siguientes valores en las columnas Nombre y Valor; de lo contrario, agregue estos valores.

Nombre	Valor
isolation.tools.copy.disable	true
isolation.tools.paste.disable	true
isolation.tools.setGUIOptions.enable	false

   Estas opciones anulan la configuración realizada en el panel de control de VMware Tools del sistema operativo invitado.

6 Haga clic en **Aceptar**.

7 (opcional) Si realizó cambios en los parámetros de configuración, reinicie la máquina virtual.

Limitar la exposición de los datos confidenciales copiados al portapapeles

De forma predeterminada, las operaciones para copiar y pegar están deshabilitadas para los hosts a fin de evitar la exposición de los datos confidenciales que se copiaron al portapapeles.

Cuando la función copiar y pegar está habilitada en una máquina virtual que ejecuta VMware Tools, se pueden copiar y pegar elementos entre el sistema operativo invitado y la consola remota. Cuando se centra la atención sobre la ventana de la consola, los procesos que se ejecutan en la máquina virtual y los usuarios sin privilegios pueden acceder al portapapeles de la consola de la máquina virtual. Si un usuario copia información confidencial en el portapapeles antes de utilizar la consola, el usuario podrá exponer datos confidenciales a la máquina virtual. Para evitar este problema, las operaciones para copiar y pegar del sistema operativo invitado están deshabilitadas de forma predeterminada.

De ser necesario, es posible habilitarlas para las máquinas virtuales.

Restringir la ejecución de comandos dentro de una máquina virtual a los usuarios

De forma predeterminada, un usuario con la función Administrador de vCenter Server puede interactuar con archivos y aplicaciones dentro del sistema operativo invitado de una máquina virtual. Para reducir el riesgo de infracciones de confidencialidad, disponibilidad o integridad del invitado, cree una función de acceso que no sea de invitado sin el privilegio **Operaciones de invitado**. Asigne esa función a los administradores que no necesiten acceso a archivos de máquinas virtuales.

Por motivos de seguridad, aplique las mismas restricciones en los permisos de acceso al centro de datos virtual que en el centro de datos físico. Aplique una función personalizada que deshabilite el acceso a invitados para usuarios que necesiten privilegios de administrador, pero que no estén autorizados a interactuar con archivos y aplicaciones del sistema operativo invitado.

Por ejemplo, la configuración puede incluir una máquina virtual en la infraestructura que tenga información confidencial.

Si tareas tales como migración con vMotion necesitan que los administradores de centros de datos puedan acceder a la máquina virtual, deshabilite algunas operaciones remotas del sistema operativo invitado para garantizar que esos administradores no puedan acceder a información confidencial.

Requisitos previos

Compruebe que tenga privilegios de **Administrador** en el sistema vCenter Server en el que crea la función.

Procedimiento

1 Inicie sesión en vSphere Client como un usuario con privilegios de **Administrador** en el sistema vCenter Server donde desea crear la función.

2 Seleccione **Administración** y haga clic en **Funciones**.

3 Haga clic en la función Administrador y haga clic en el icono **Clonar acción de función**.

4 Introduzca un nombre de función y una descripción, y haga clic en **Aceptar**.

   Por ejemplo, escriba `Administrator No Guest Access`.

5 Seleccione la función clonada y haga clic en el icono **Editar acción de función**.

6 En el privilegio **Máquina virtual**, anule la selección de **Operaciones de invitados** y haga clic en **Siguiente**.

7 Haga clic en **Finalizar**.

Pasos siguientes

Seleccione el sistema vCenter Server o el host, y asigne un permiso que se asocie con el usuario o el grupo que debe tener los nuevos privilegios con la función recién creado. Quite esos usuarios de la función Administrador.

Evitar que un usuario o proceso de máquina virtual desconecten dispositivos

Los usuarios y los procesos sin privilegios de raíz o administrador en máquinas virtuales pueden conectar o desconectar dispositivos, como adaptadores de red y unidades de CD-ROM, y pueden modificar la configuración de los dispositivos. Para mejorar la seguridad de la máquina virtual, quite estos dispositivos.

Puede evitar que los usuarios de la máquina virtual en el sistema operativo invitado y los procesos que se ejecutan en el sistema operativo invitado modifiquen los dispositivos mediante cambios en la configuración avanzada de la máquina virtual.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Seleccione **Opciones de máquina virtual**.

4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.

5 Compruebe que se detallen los siguientes valores en las columnas Nombre y Valor; de lo contrario, agregue estos valores.

Nombre	Valor
isolation.device.connectable.disable	true
isolation.device.edit.disable	true

   Esta configuración no afecta la capacidad de un administrador de vSphere para conectar o desconectar los dispositivos asociados a la máquina virtual.

6 Haga clic en **Aceptar** para cerrar el cuadro de diálogo Parámetros de configuración y, a continuación, haga clic nuevamente en **Aceptar**.

Evitar que los procesos del sistema operativo invitado envíen mensajes de configuración al host

Para asegurarse de que el sistema operativo invitado no modifique los parámetros de configuración, se puede evitar que estos procesos escriban cualquier par nombre-valor en el archivo de configuración.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Seleccione **Opciones de máquina virtual**.

4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.

5 Haga clic en **Agregar parámetros de configuración** e introduzca los siguientes valores en las columnas Nombre y Valor.

Columna	Valor
Nombre	`isolation.tools.setinfo.disable`
Valor	`true`

6 Haga clic en **Aceptar** para cerrar el cuadro de diálogo Parámetros de configuración y, a continuación, haga clic nuevamente en **Aceptar**.

Evitar utilizar discos independientes no persistentes

Al utilizar discos independientes no persistentes, los atacantes exitosos pueden apagar o reiniciar el sistema y así eliminar cualquier evidencia de que la máquina fue vulnerada. Sin un registro persistente de la actividad de la máquina virtual, los administradores podrían desconocer el ataque. Por lo tanto, debe evitar utilizar discos independientes no persistentes.

Procedimiento

◆ Asegúrese de que la actividad de la máquina virtual se registre de forma remota en un servidor separado, como un servidor syslog o un recopilador de eventos basado en Windows.

  Si el registro remoto de eventos y de actividad no está configurado para el invitado, el modo scsiX:Y. debe estar configurado de alguna de las siguientes formas:

  - No presente

- No establecido en independiente no persistente

Resultados

Cuando el modo no persistente no está habilitado, no se puede revertir la máquina virtual a un estado conocido al reiniciar el sistema.

Cifrado de máquinas virtuales 6

A partir de vSphere 6.5, puede aprovechar el cifrado de máquinas virtuales. El cifrado no solo protege la máquina virtual, sino también los discos de las máquinas virtuales y otros archivos. Si establece una conexión de confianza entre vCenter Server y un servidor de administración de claves (key management server, KMS), vCenter Server puede recuperar claves del KMS, si fuera necesario.

Los distintos aspectos del cifrado de máquinas virtuales se administran de diversas maneras.

- Administre la instalación de una conexión de confianza con el KMS y realice la mayoría de los flujos de trabajo de cifrado de vSphere Client.
- Administre la automatización de algunas funciones avanzadas de vSphere Web Services SDK. Consulte *Guía de programación de vSphere Web Services SDK* y *Referencia de VMware vSphere API*.
- Utilice la herramienta de línea de comandos `crypto-util` directamente en el host ESXi en algunos casos especiales, por ejemplo, para descifrar volcados de núcleo de un paquete de `vm-support`.

Descripción general del cifrado de máquinas virtuales de vSphere (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_4f7i39o8/uiConfId/49694343/)

Este capítulo incluye los siguientes temas:

- Cómo el cifrado de máquinas virtuales de vSphere protege el entorno
- Componentes de cifrado de máquinas virtuales de vSphere
- Flujo del proceso de cifrado
- Cifrado de disco virtual
- Requisitos previos y privilegios necesarios para tareas de cifrado
- vSphere vMotion cifrado
- Interoperabilidad, advertencias y prácticas recomendadas de cifrado

Cómo el cifrado de máquinas virtuales de vSphere protege el entorno

Con el cifrado de máquinas virtuales de vSphere, puede crear máquinas virtuales cifradas y cifrar máquinas virtuales existentes. Debido a que se cifran todos los archivos de máquinas virtuales con información confidencial, la máquina virtual está protegida. Solo los administradores con privilegios de cifrado puede realizar tareas de cifrado y descifrado.

Claves utilizadas

Se usan dos tipos de claves para el cifrado.

- El host ESXi genera y usa claves internas para cifrar máquinas y discos virtuales. Estas claves se usan como claves de cifrado de datos (Data Encryption Keys, DEK) y son claves XTS-AES-256.
- vCenter Server le solicita claves al KMS. Estas claves se usan como la clave de cifrado de claves (key encryption key, KEK), y son claves AES-256. vCenter Server almacena solo el identificador de cada KEK, pero no la clave en sí.
- ESXi utiliza la KEK para cifrar las claves internas y almacena la clave interna cifrada en el disco. ESXi no almacena la KEK en el disco. Si un host se reinicia, vCenter Server solicita la KEK con el identificador correspondiente del KMS y la pone a disposición de ESXi. De este modo, ESXi puede descifrar las claves internas según sea necesario.

Elementos cifrados

El cifrado de máquinas virtuales de vSphere admite el cifrado de archivos de máquinas virtuales, archivos de discos virtuales y archivos de volcados de núcleo.

Archivos de la máquina virtual

Se cifra la mayoría de los archivos de máquinas virtuales, en particular los datos de invitados que no se almacenan en el archivo VMDK. Este conjunto de archivos incluye, entre otros, los archivos de NVRAM, VSWP y VMSN. La clave que vCenter Server recupera de KMS desbloquea un paquete cifrado en el archivo VMX que contiene claves internas y otros secretos.

Si utiliza vSphere Client para crear una máquina virtual cifrada, puede cifrar y descifrar discos virtuales de manera independiente de los archivos de máquinas virtuales. Si utiliza vSphere Web Client para crear una máquina virtual cifrada, todos los discos virtuales se cifran de manera predeterminada. Para otras tareas de cifrado, en ambos clientes, como el cifrado de una máquina virtual existente, puede cifrar y descifrar discos virtuales de manera independiente de los archivos de máquinas virtuales.

Nota No se puede asociar un disco virtual cifrado con una máquina virtual que no está cifrada.

Archivos de disco virtual

Los datos de un archivo de disco virtual cifrado (VMDK) jamás se escriben en texto no cifrado en el almacenamiento o el disco físico, ni tampoco se transmiten por la red en texto no cifrado. El archivo de descriptor de VMDK incluye en su mayoría texto no cifrado, pero contiene un identificador de clave para la KEK y la clave interna (DEK) en el paquete cifrado.

Puede usar vSphere API para realizar una operación de repetición de cifrado superficial con una nueva KEK, o bien una operación de repetición de cifrado profunda con una nueva clave interna.

Volcados de núcleos

Los volcados de núcleo en un host ESXi en el que se habilitó el modo de cifrado siempre están cifrados. Consulte Cifrado de máquinas virtuales de vSphere y volcados de núcleo.

Nota Los volcados de núcleo en el sistema vCenter Server no están cifrados. Proteja el acceso al sistema vCenter Server.

Nota Para obtener información sobre algunas limitaciones relacionadas con dispositivos y características con las que puede interoperar el cifrado de máquinas virtuales de vSphere, consulte Interoperabilidad del cifrado de máquinas virtuales.

Elementos no cifrados

Algunos de los archivos relacionados con una máquina virtual no se cifran o se cifran parcialmente.

Archivos de registro

Los archivos de registro no se cifran, ya que no contienen datos confidenciales.

Archivos de configuración de máquinas virtuales

La mayoría de la información de configuración de máquinas virtuales, almacenada en los archivos VMX y VMSD, no está cifrada.

Archivo de descriptor de discos virtuales

Para admitir la administración de discos sin una clave, la mayor parte del archivo de descriptor de discos virtuales no se cifra.

Usuarios que pueden realizar operaciones de cifrado

Solo los usuarios a los que se asignan privilegios de **Operaciones criptográficas** pueden realizar operaciones criptográficas. El conjunto de privilegios tiene una granularidad fina. Consulte Privilegios de operaciones de cifrado. La función del sistema predeterminada Administrador incluye todos los privilegios de **Operaciones criptográficas**. Una nueva función, Sin administrador de criptografía, admite todos los privilegios de Administrador, salvo los privilegios de **Operaciones criptográficas**.

Puede crear funciones personalizadas adicionales, por ejemplo, para permitir que un grupo de usuarios cifre máquinas virtuales, pero impedirles que las descifren.

Realización de operaciones de cifrado

vSphere Client y vSphere Web Client admiten muchas de las operaciones criptográficas. Para otras tareas, puede usar vSphere API.

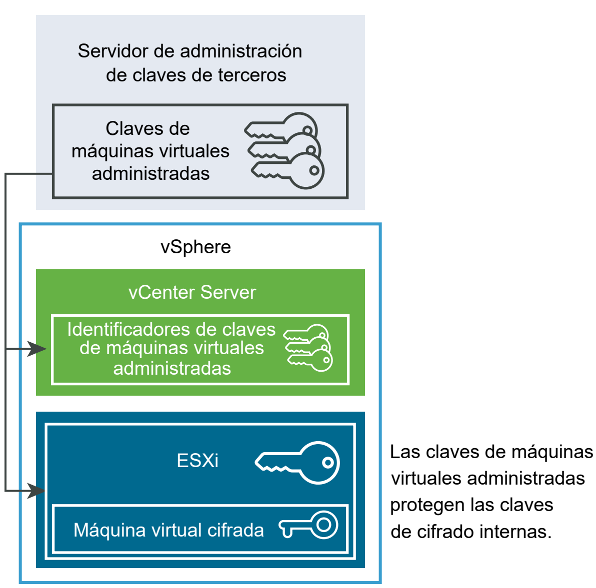
Tabla 6-1. Interfaces para realizar operaciones de cifrado

Interfaz	Operaciones	Información
vSphere Client o vSphere Web Client	Crear una máquina virtual cifrada Cifrar y descifrar máquinas virtuales	Este libro.
vSphere Web Services SDK	Crear una máquina virtual cifrada Cifrar y descifrar máquinas virtuales Realice una operación de repetición de cifrado profunda de una máquina virtual (con otra DEK). Realice una operación de repetición de cifrado superficial de una máquina virtual (con otra KEK).	*Guía de programación de vSphere Web Services SDK* *Referencia de VMware vSphere API*
`crypto-util`	Descifre volcados de núcleo cifrados, compruebe si los archivos están cifrados y realice otras tareas de administración directamente en el host ESXi.	Ayuda de línea de comandos. Cifrado de máquinas virtuales de vSphere y volcados de núcleo

Componentes de cifrado de máquinas virtuales de vSphere

Un KMS externo, el sistema vCenter Server y los hosts ESXi contribuyen a la solución de cifrado de máquinas virtuales de vSphere.

Figura 6-1. Arquitectura del cifrado virtual de vSphere



Servidor de administración de claves

vCenter Server solicita claves de un KMS externo. El KMS genera y almacena las claves, y después las envía a vCenter Server para su distribución.

Puede utilizar vSphere Web Client o vSphere API para agregar un clúster de instancias de KMS al sistema vCenter Server. Si utiliza varias instancias de KMS en un clúster, todas las instancias deben ser del mismo proveedor y deben replicar claves.

Si el entorno utiliza distintos proveedores de KMS en distintos entornos, puede agregar un clúster de KMS para cada KMS y especificar un clúster de KMS predeterminado. El primer clúster que agrega se convertirá en el clúster predeterminado. Podrá especificar explícitamente el predeterminado más adelante.

Como cliente de KMIP, vCenter Server utiliza un protocolo de interoperabilidad de administración de claves (Key Management Interoperability Protocol, KMIP) para que sea sencillo utilizar el KMS que el usuario desea.

vCenter Server

Solo vCenter Server tiene las credenciales para registrarse en el KMS. Los hosts ESXi no tienen esas credenciales. vCenter Server obtiene las claves del KMS y las inserta en los hosts ESXi. vCenter Server no almacena las claves del KMS, pero sí conserva una lista de identificadores de claves.

vCenter Server comprueba los privilegios de los usuarios que realizan operaciones de cifrado. Puede utilizar vSphere Web Client para asignar privilegios de operaciones de cifrado o para asignar la función personalizada **Sin administrador de criptografía** a grupos de usuarios. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado.

vCenter Server agrega eventos de cifrado a la lista de eventos que se pueden ver y exportar de la consola de eventos de vSphere Web Client. Cada evento incluye el usuario, la hora, el identificador de clave y la operación de cifrado.

Las claves que provienen del KMS se utilizan como claves de cifrado de claves (key encryption key, KEK).

Hosts ESXi

Los hosts ESXi se encargan de diversos aspectos del flujo de trabajo de cifrado.

- vCenter Server introduce claves en un host ESXi cuando el host necesita una clave. El host debe tener habilitado el modo de cifrado. La función actual del usuario debe contar con privilegios de operaciones de cifrado. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado y Privilegios de operaciones de cifrado.
- Garantizar que los datos del invitado de las máquinas virtuales cifradas estén cifrados cuando se almacenan en el disco.
- Garantizar que los datos del invitado de las máquinas virtuales cifradas no se envíen a la red sin cifrar.

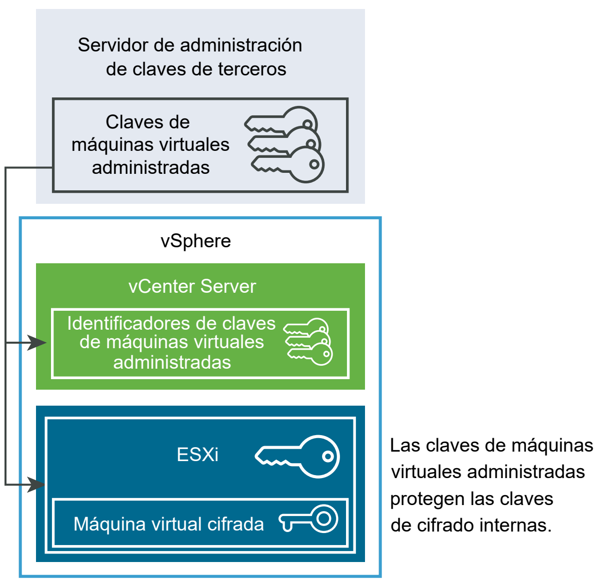
Las claves que generan los hosts ESXi se denominan claves internas en este documento. Estas claves, por lo general, actúan como claves de cifrado de datos (Data Encryption Key, DEK).

Flujo del proceso de cifrado

Después de que vCenter Server se conecta con el KMS, los usuarios que tengan los privilegios necesarios pueden crear máquinas y discos virtuales cifrados. Tales usuarios también pueden realizar otras tareas de cifrado, como cifrar máquinas virtuales existentes y descifrar máquinas virtuales cifradas.

El flujo del proceso incluye el KMS, vCenter Server y el host de ESXi.

Figura 6-2. Arquitectura del cifrado virtual de vSphere



Durante el proceso de cifrado, los distintos componentes de vSphere interactúan del siguiente modo.

1 Cuando el usuario realiza una tarea de cifrado, por ejemplo, crear una máquina virtual cifrada, vCenter Server solicita una nueva clave del KMS predeterminado. Esta clave se utilizará como la KEK.

2 vCenter Server almacena el identificador de la clave y pasa la clave al host ESXi. Si el host ESXi es parte del clúster, vCenter Server envía la KEK a cada host del clúster.

   La clave en sí no se guarda en el sistema de vCenter Server. Solo se conoce el identificador de la clave.

3 El host ESXi genera claves internas (DEK) para la máquina virtual y sus discos. Mantiene las claves internas solo en la memoria y usa las KEK para cifrar las claves internas.

   Nunca se guardan en el disco las claves internas sin cifrar. Solo se guardan los datos cifrados. Dado que las KEK provienen del KMS, el host sigue usando las mismas KEK.

4 El host ESXi cifra la máquina virtual con la clave interna cifrada.

Todos los hosts que tengan la KEK y puedan acceder al archivo de la clave cifrada pueden realizar operaciones en la máquina o el disco virtual cifrado.

Si posteriormente desea descifrar una máquina virtual, puede cambiar su directiva de almacenamiento. Puede cambiar la directiva de almacenamiento de la máquina virtual y todos los discos. Si desea descifrar un componente individual, descifre primero el componente seleccionado y luego descifre la máquina virtual cambiando la directiva de almacenamiento para el inicio de la máquina virtual. Ambas claves son necesarias para descifrar cada uno de los componentes.

Cifrar máquinas y discos virtuales (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_rndb367u/uiConfId/49694343/)

Cifrado de disco virtual

Cuando se crea una máquina virtual cifrada a partir de vSphere Client, puede decidir qué discos se excluirán del cifrado. Cuando crea una máquina virtual cifrada desde vSphere Web Client, se cifran todos los discos virtuales. Posteriormente, puede agregar discos y establecer sus directivas de cifrado. No se puede agregar un disco cifrado a una máquina virtual que no está cifrada y no se puede cifrar un disco si la máquina virtual no está cifrada.

El cifrado de una máquina virtual y de sus discos se controla mediante directivas de almacenamiento. La directiva de almacenamiento de inicio de la máquina virtual rige la propia máquina, virtual y cada disco virtual tiene una directiva de almacenamiento asociada.La directiva de almacenamiento de inicio de la máquina virtual rige la propia máquina, y cada disco virtual tiene una directiva de almacenamiento asociada.

- Al definir la directiva de almacenamiento de inicio de la máquina virtual con una directiva de cifrado, solo se cifra la máquina virtual.
- Al definir la directiva de almacenamiento de inicio de la máquina virtual y de todos los discos con una directiva de cifrado, se cifran todos los componentes.

Tenga en cuenta los siguientes casos de uso.

Tabla 6-2. Casos de uso de cifrado de discos virtuales

Caso de uso	Detalles
Cree una máquina virtual cifrada.	Si agrega discos al crear una máquina virtual cifrada, los discos se cifran de manera predeterminada. Puede cambiar la directiva de manera que no se cifren uno o más discos. Después de la creación de una máquina virtual, puede cambiar explícitamente la directiva de almacenamiento de cada disco. Consulte Cambiar la directiva de cifrado para discos virtuales.
Cifre una máquina virtual.	Para cifrar una máquina virtual actual, debe cambiar la directiva de almacenamiento.Para cifrar una máquina virtual, debe cambiar la directiva de almacenamiento. Se puede cambiar la directiva de almacenamiento de la máquina virtual y de todos los discos virtuales. Para cifrar solo la máquina virtual, puede especificar una directiva de cifrado para el inicio de la máquina virtual y seleccionar una directiva de almacenamiento diferente para cada disco virtual (por ejemplo, Valor predeterminado de almacén de datos). Consulte Crear una máquina virtual cifrada.
Agregue un disco sin cifrar existente a la máquina virtual cifrada (directiva de almacenamiento de cifrado).	Se produce un error. Debe agregar el disco con la directiva de almacenamiento predeterminada, pero luego puede cambiar la directiva de almacenamiento. Consulte Cambiar la directiva de cifrado para discos virtuales.
Agregar un disco sin cifrar actual a una máquina virtual cifrada con una directiva de almacenamiento que no incluye cifrado, por ejemplo, Valor predeterminado de almacén de datos.	El disco utiliza la directiva de almacenamiento predeterminada. Puede cambiar de manera explícita la directiva de almacenamiento después de agregar el disco si desea un disco cifrado. Consulte Cambiar la directiva de cifrado para discos virtuales.
Agregar un disco cifrado a una máquina virtual cifrada. La directiva de almacenamiento del inicio de la máquina virtual es Cifrado.	Cuando agrega el disco, este permanece cifrado. vSphere Web Client muestra el tamaño y otros atributos, incluso el estado de cifrado, pero puede que no muestre la directiva de almacenamiento correcta. Para mantener la coherencia, cambie la directiva de almacenamiento.
Agregar un disco cifrado actual a una máquina virtual sin cifrar.	Este caso de uso no es compatible.

Requisitos previos y privilegios necesarios para tareas de cifrado

Las tareas de cifrado son solo posibles en los entornos que incluyen vCenter Server. Además, el host ESXi debe tener un modo de cifrado habilitado para la mayoría de las tareas de cifrado. El usuario que realiza la tarea debe contar con los privilegios correspondientes. Un conjunto de privilegios **Operaciones criptográficas** permite un control detallado. Si las tareas de cifrado de máquinas virtuales requieren un cambio en el modo de cifrado de host, se requieren privilegios adicionales.

Privilegios de cifrado y funciones

De manera predeterminada, el usuario con la función Administrador de vCenter Servertiene todos los privilegios. La función **Sin administrador de criptografía** no tiene los siguientes privilegios que se requieren para las operaciones de cifrado.

- Agregue los privilegios **Operaciones criptográficas**.
- **Global.Diagnósticos**
- **Host.Inventario.Agregar host a clúster**
- **Host.Inventario.Agregar host independiente**
- **Host.Operaciones locales.Administrar grupos de usuarios**

Puede asignar la función **Sin administrador de criptografía** para los administradores de vCenter Server que no necesitan privilegios **Operaciones criptográficas**.

Para limitar aún más lo que pueden hacer los usuarios, puede clonar la función **Sin administrador de criptografía** y crear una función personalizada solo con algunos privilegios **Operaciones criptográficas**. Por ejemplo, puede crear una función que permita a los usuarios cifrar máquinas virtuales, pero no descifrarlas. Consulte Usar funciones para asignar privilegios.

Modo de cifrado de host

El modo de cifrado de host determina si un host ESXi está listo para aceptar material de cifrado con el fin de cifrar las máquinas virtuales y los discos virtuales. Para realizar las operaciones de cifrado en un host, debe habilitarse el modo de cifrado de host. El modo de cifrado de host a menudo se habilita automáticamente, pero también puede habilitarse de forma explícita. Puede comprobar y establecer de forma intencional el modo de cifrado de host actual desde vSphere Client o mediante vSphere API.

Cuando se habilita el modo de cifrado de host, vCenter Server instala una clave de host en el host, lo que garantiza que este está "seguro" desde el punto de vista del cifrado. Tras establecer la clave de host, se pueden realizar otras operaciones de cifrado, incluidas la obtención por parte de vCenter Server de claves del clúster del servidor de administración de claves y la inserción de estas en los hosts ESXi.

En el modo "seguro", se cifran los volcados de núcleos de los ámbitos de usuario (es decir, hostd) y las máquinas virtuales cifradas. No se cifran los volcados de núcleos de las máquinas virtuales sin cifrar.

Para obtener más información sobre los volcados de núcleos cifrados y la forma en que los utiliza el soporte técnico de VMware, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2147388.

Para obtener instrucciones, consulte Habilitar el modo de cifrado de host de forma explícita.

Una vez que el modo de cifrado de host está habilitado, no puede deshabilitarse con facilidad. Consulte Deshabilitar el modo de cifrado de host.

Los cambios automáticos se producen cuando las operaciones de cifrado intentan habilitar el modo de cifrado de host. Por ejemplo, supongamos se agrega una máquina virtual cifrada a un host independiente y que el modo de cifrado de host no está habilitado. Si se tienen los privilegios correspondientes en el host, el modo de cifrado cambia a habilitado en forma automática.

Supongamos que el clúster tiene tres hosts ESXi: A, B y C. Debe crear una máquina virtual cifrada en el host A. Lo que suceda dependerá de varios factores.

- Si ya se ha habilitado el cifrado para los hosts A, B y C, solo se necesitan los privilegios **Operaciones criptográficas.Cifrar nuevo** para crear la máquina virtual.
- Si los hosts A y B están habilitados para el cifrado y el C no lo está, el sistema procede de la siguiente manera.
  - Supongamos que tiene los privilegios **Operaciones criptográficas.Cifrar nuevo** y los privilegios **Operaciones de cifrado.Registrar host** en cada host. En ese caso, el proceso de creación de la máquina virtual habilitará el cifrado en el host C. El proceso de cifrado habilitará el modo de cifrado de hosts en el host C y envíará la clave a cada host del clúster.

    Para este caso, también se puede habilitar el cifrado de host en el host C de forma explícita.
  - Suponga que solo tiene los privilegios **Operaciones criptográficas.Cifrar nuevo** en la máquina virtual o en una carpeta de máquinas virtuales. En ese caso, la creación de máquinas virtuales se completará correctamente y la clave estará disponible en el host A y el host B. El host C permanecerá deshabilitado para el cifrado y no tendrá la clave de la máquina virtual.
- Si ninguno de los hosts tiene el cifrado habilitado y cuenta con los privilegios **Operaciones criptográficas.Registrar host** en el host A, el proceso de creación de la máquina virtual habilitará el cifrado de hosts en dicho host. De lo contrario, se produce un error.

Requisitos de espacio de disco

Al cifrar una máquina virtual existente, se necesita al menos el doble de espacio que el que utiliza actualmente la máquina virtual.

vSphere vMotion cifrado

A partir de vSphere 6.5, vSphere vMotion siempre utiliza el cifrado para migrar máquinas virtuales cifradas. Para las máquinas virtuales sin cifrar, se puede seleccionar una de las opciones de vSphere vMotion cifrado.

vSphere vMotion cifrado garantiza la confidencialidad, la integridad y la autenticidad de los datos que se transfieren con vSphere vMotion.

- vSphere admite vMotion cifrado de máquinas virtuales sin cifrar entre instancias de vCenter Server.

- vSphere no admite vMotion de máquinas virtuales cifradas entre instancias de vCenter Server. Debido a que una instancia de vCenter no puede comprobar si otra instancia de vCenter está conectada al mismo clúster del sistema de administración de claves, las claves de cifrado adecuadas no están disponibles para realizar correctamente una operación de cifrado de máquina virtual. Por ello, actualmente no se admite una instancia de vMotion en estas circunstancias.

Elementos cifrados

En los discos cifrados, los datos se transmiten cifrados. En los discos sin cifrar, no se admite el cifrado de Storage vMotion.

En las máquinas virtuales cifradas, siempre se utiliza vSphere vMotion cifrado para la migración con vSphere vMotion. No se puede desactivar vSphere vMotion cifrado en las máquinas virtuales cifradas.

Estados de vSphere vMotion cifrado

En las máquinas virtuales sin cifrar, se puede establecer vSphere vMotion cifrado en uno de los siguientes estados. El valor predeterminado es Oportunista.

Deshabilitado

No se utiliza vSphere vMotion cifrado.

Oportunista

Se utiliza vSphere vMotion cifrado si los hosts de origen y destino lo admiten. Solo ESXi 6.5 y las versiones posteriores utilizan vSphere vMotion cifrado.

Obligatorio

Solo se permite vSphere vMotion cifrado. Si el host de origen o de destino no admite vSphere vMotion cifrado, no se permite la migración con vSphere vMotion.

Cuando se cifra una máquina virtual, la máquina virtual conserva un registro de la configuración actual de vSphere vMotion cifrado. Si posteriormente se deshabilita el cifrado para la máquina virtual, la configuración de vMotion cifrado sigue siendo Obligatorio hasta que se modifica de forma explícita la configuración. Es posible modificar la configuración mediante la opción **Editar configuración**.

Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la forma de habilitar y deshabilitar vSphere vMotion cifrado en máquinas virtuales sin cifrar.

Interoperabilidad, advertencias y prácticas recomendadas de cifrado

Todas las prácticas recomendadas y las advertencias correspondientes al cifrado de máquinas físicas se aplican también al cifrado de máquinas virtuales. La arquitectura de cifrado de máquinas

virtuales presenta algunas recomendaciones adicionales. Tenga en cuenta las limitaciones de interoperabilidad al planear su estrategia de cifrado de máquinas virtuales.

Prácticas recomendadas de cifrado de máquinas virtuales

Siga las prácticas recomendadas de cifrado de máquinas virtuales para evitar problemas futuros, por ejemplo, al generar un paquete de `vm-support`.

Prácticas recomendadas generales

Siga estas prácticas recomendadas generales para evitar problemas.

- No cifre ninguna máquina virtual de vCenter Server Appliance.
- Si se produce un error en el host ESXi, recupere el paquete de soporte lo antes posible.
  La clave de host debe estar disponible para generar un paquete de soporte que utilice una contraseña o para descifrar un volcado de núcleo. Si el host se reinicia, es posible que se cambie la clave de host. En caso de que esto suceda, ya no se podrá generar un paquete de soporte con una contraseña ni descifrar volcados de núcleo en el paquete de soporte con la clave de host.
- Administre los nombres de clúster del KMS con cuidado. Si cambia el nombre de clúster de un KMS por un KMS que ya está en uso, la máquina virtual cifrada con las claves de ese KMS pasa a tener el estado bloqueado durante el encendido o el registro. En ese caso, elimine el KMS de vCenter Server y agréguelo con el nombre de clúster que utilizó al comienzo.
- No edite los archivos VMX ni los archivos de descriptores de VMDK. Estos archivos contienen el paquete de cifrado. Es posible que la máquina virtual no se pueda recuperar debido a los cambios realizados y que el problema de recuperación no se pueda solucionar.
- El proceso de cifrado cifra los datos del host antes de que se escriban en el almacenamiento. Las funciones de almacenamiento de back-end, como la desduplicación y la compresión, pueden no ser efectivas para las máquinas virtuales cifradas. Al usar el cifrado de máquinas virtuales de vSphere, tenga en cuenta los compromisos de almacenamiento.
- El cifrado requiere gran consumo de CPU. AES-NI mejora significativamente el rendimiento del cifrado. Habilite AES-NI en el BIOS.

Prácticas recomendadas para volcados de núcleo cifrados

Siga estas prácticas recomendadas para evitar problemas cuando desee examinar un volcado de núcleo a fin de diagnosticar un problema.

- Establezca una directiva con respecto a los volcados de núcleo. Los volcados de núcleo están cifrados porque pueden contener información confidencial, por ejemplo, claves. Si descifra un volcado de núcleo, asuma que contiene información confidencial. Los volcados de núcleo de ESXi pueden contener claves para el host ESXi y para las máquinas virtuales que este contiene. Después de descifrar un volcado de núcleo, considere cambiar la clave del host y volver a cifrar las máquinas virtuales cifradas. Puede realizar ambas tareas con vSphere API.

Consulte Cifrado de máquinas virtuales de vSphere y volcados de núcleo para obtener detalles.

- Siempre utilice una contraseña cuando recopile un paquete de `vm-support`. Puede especificar la contraseña cuando genera el paquete de soporte de vSphere Client o puede utilizar el comando `vm-support`.

  La contraseña vuelve a cifrar los volcados de núcleo que utilizan claves internas de manera que estos volcados empleen claves basadas en la contraseña. Posteriormente, se puede usar la contraseña para descifrar cualquier volcado de núcleo cifrado que pudiera estar incluido en el paquete de soporte. El uso de la opción de contraseña no afecta a los volcados de núcleo sin cifrar ni los registros.

- La contraseña que especificó durante la creación del paquete de `vm-support` no persiste en los componentes de vSphere. Es su responsabilidad llevar un registro de las contraseñas de los paquetes de soporte.
- Antes de cambiar la clave de host, genere un paquete de soporte de la máquina virtual con una contraseña. Más adelante, puede usar la contraseña para acceder a todos los volcados de núcleo que se hayan cifrado con la clave de host anterior.

Prácticas recomendadas para la administración del ciclo de vida de claves

Implemente prácticas recomendadas que garanticen la disponibilidad del KMS y supervise claves en el KMS.

- Es su responsabilidad implementar directivas que garanticen la disponibilidad del KMS.

  Si el KMS no está disponible, no se pueden realizar operaciones de máquinas virtuales que requieren que vCenter Server solicite la clave del KMS. Eso significa que las máquinas virtuales en ejecución siguen ejecutándose, y puede encenderlas, apagarlas y volver a configurarlas. No obstante, no puede reubicar la máquina virtual en un host que no tiene la información de la clave.

  La mayoría de las soluciones de KMS incluyen funciones de alta disponibilidad. Puede utilizar vSphere Client o la API para especificar un clúster de KMS y los servidores de KMS asociados.

- Es su responsabilidad llevar un registro de las claves y encontrar soluciones si las claves de las máquinas virtuales actuales no tienen el estado Activa.

  El estándar KMIP define los siguientes estados para las claves:

  - Preactiva
  - activa
  - Desactivada
  - Comprometida
  - Destruida
  - Comprometida destruida

El cifrado de máquinas virtuales de vSphere utiliza solo claves con el estado Activa para cifrar. Si la clave está en el estado Preactiva, el cifrado de máquinas virtuales de vSphere la activa. Si el estado de la clave es Desactivada, Comprometida, Destruida o Comprometida destruida, no se pueden cifrar una máquina ni un disco virtuales con esa clave.

Las máquinas virtuales que usan estas claves seguirán funcionando cuando las claves tengan otros estados. La correcta ejecución de una operación de clonación o migración dependerá de si la clave ya existe en el host.

- Si la clave existe en el host de destino, la operación se realiza correctamente incluso si la clave no tiene el estado Activa en el KMS.
- Si las claves de máquina virtual y disco virtual no están en el host de destino, vCenter Server debe recuperar las claves del KMS. Si el estado de la clave es Desactivada, Comprometida, Destruida o Comprometida destruida, vCenter Server muestra un error y la operación no se realiza correctamente.

Una operación de clonación o de migración se realiza correctamente si la clave ya está en el host. Se produce un error en la operación si vCenter Server debe extraer las claves del KMS.

Si una clave no tiene el estado Activa, vuelva a introducir la clave con la API. Consulte la *Guía de programación de vSphere Web Services SDK*.

Prácticas recomendadas de copia de seguridad y restauración

Establezca directivas para las operaciones de copias de seguridad y restauración.

- No todas las arquitecturas de copias de seguridad son compatibles. Consulte Interoperabilidad del cifrado de máquinas virtuales.
- Establezca directivas para las operaciones de restauración. Debido a que las copias de seguridad siempre incluyen texto no cifrado, cifre las máquinas virtuales inmediatamente después de que finalice la restauración. Puede especificar que se cifre la máquina virtual como parte de la operación de restauración. Si fuera posible, cifre la máquina virtual como parte del proceso de restauración para evitar que se divulgue información confidencial. Para cambiar la directiva de cifrado de cualquier disco que esté relacionado con la máquina virtual, cambie la directiva de almacenamiento de ese disco.
- Debido a que los archivos de inicio de la máquina virtual están cifrados, asegúrese de que las claves de cifrado estén disponibles en el momento de una restauración.

Prácticas recomendadas de rendimiento

- El rendimiento del cifrado depende de la velocidad de la CPU y del almacenamiento.
- El cifrado de las máquinas virtuales existentes lleva más tiempo que el cifrado de una máquina virtual durante la creación. En lo posible, cifre la máquina virtual al crearla.

Prácticas recomendadas de directivas de almacenamiento

No modifique la directiva de almacenamiento de muestra de cifrado de una máquina virtual en paquete. En lugar de ello, clone la directiva y edite el clon.

Nota No existe ninguna manera automatizada de restaurar la directiva de cifrado de una máquina virtual a la configuración original.

Consulte la documentación de *Almacenamiento de vSphere* si desea obtener información para personalizar las directivas de almacenamiento.

Advertencias de cifrado de máquinas virtuales

Revise las advertencias de cifrado de máquinas virtuales para evitar problemas futuros.

Si desea comprender qué dispositivos y funciones no se pueden usar con el cifrado de máquinas virtuales, consulte Interoperabilidad del cifrado de máquinas virtuales.

Limitaciones

Tenga en cuenta las siguientes advertencias cuando planifique una estrategia de cifrado de máquinas virtuales.

- Cuando clona una máquina virtual cifrada o realiza una operación de Storage vMotion, puede intentar cambiar el formato del disco. Esas conversiones no siempre se realizan correctamente. Por ejemplo, si clona una máquina virtual e intenta cambiar el disco de un formato grueso sin puesta a cero diferido a un formato fino, el disco de la máquina virtual conserva el formato grueso sin puesta a cero diferido.
- Si separa un disco de una máquina virtual, no se conservará la información de la directiva de almacenamiento del disco virtual.
  - Si el disco virtual está cifrado, debe establecer explícitamente la directiva de almacenamiento en la directiva de cifrado de la máquina virtual o en una directiva de almacenamiento que incluya el cifrado.
  - Si el disco virtual no está cifrado, puede cambiar la directiva de almacenamiento cuando agrega el disco a la máquina virtual.

  Consulte Cifrado de disco virtual para obtener detalles.
- Descifre los volcados de núcleo antes de mover una máquina virtual a un clúster diferente.

  vCenter Server no almacena las claves del KMS, solo realiza seguimiento de los identificadores de claves. Por este motivo, vCenter Server no almacena claves de hosts ESXi de forma persistente.

  En determinadas circunstancias, por ejemplo, si mueve el host ESXi a un clúster distinto y reinicia el host, vCenter Server asigna una clave nueva al host. No se puede descifrar ningún volcado de núcleo actual con la clave de host nueva.
- Una máquina virtual cifrada no admite la exportación de OVF.

- No se admite el uso de VMware Host Client para registrar una máquina virtual cifrada.

Estado bloqueado de una máquina virtual

Si falta la clave de la máquina virtual, o una o más claves del disco virtual, la máquina virtual entra en un estado bloqueado. En un estado bloqueado, no se pueden realizar operaciones de máquinas virtuales.

- Si cifra una máquina virtual y sus discos desde vSphere Client, se utiliza la misma clave en ambos casos.
- Si realiza el cifrado con la API, puede usar distintas claves de cifrado para la máquina virtual y los discos. En un caso así, si intenta encender una máquina virtual y falta una de las claves de disco, no podrá concretar la operación de encendido. Si retira el disco virtual, podrá encender la máquina virtual.

Consulte Resolver problemas de claves faltantes si desea obtener sugerencias de solución de problemas.

Interoperabilidad del cifrado de máquinas virtuales

El cifrado de máquinas virtuales de vSphere tiene algunas limitaciones respecto de los dispositivos y las funciones con los que puede interoperar en vSphere 6.5 y versiones posteriores.

Las siguientes limitaciones y comentarios hacen referencia al uso del cifrado de máquinas virtuales de vSphere. Para obtener información similar sobre cómo usar el cifrado de vSAN, consulte la documentación de *Administrar VMware vSAN*.

Limitaciones de ciertas tareas de cifrado

Se aplican algunas restricciones al realizar ciertas tareas en una máquina virtual cifrada.

- No puede realizar la mayoría de operaciones de cifrado en una máquina virtual encendida. La máquina virtual debe estar apagada. Se puede clonar una máquina virtual cifrada y se puede realizar un cifrado superficial mientras la máquina virtual está encendida.
- No se puede realizar una repetición de cifrado profundo en una máquina virtual con instantáneas. Puede realizar una repetición de cifrado superficial en una máquina virtual con instantáneas.

Dispositivos del módulo de plataforma de confianza virtual y cifrado de máquinas virtuales de vSphere

Un módulo de plataforma de confianza virtual (virtual Trusted Platform Module, vTPM) es una representación basada en software de un chip de módulo de plataforma de confianza 2.0 físico. Se puede agregar un vTPM a una máquina virtual nueva o existente. Para agregar un vTPM a una máquina virtual, debe configurar un servidor de administración de claves (key management

server, KMS) en el entorno de vSphere. Cuando se configura un vTPM, se cifran los archivos de "inicio" de la máquina virtual (intercambio de memoria, archivos de NVRAM, etc.). Los archivos de disco, o archivos VMDK, no se cifran automáticamente. Puede optar por agregar el cifrado de forma explícita para los discos de la máquina virtual.

Precaución Al clonar una máquina virtual, se duplica toda la máquina virtual, incluidos los dispositivos virtuales, como un vTPM. También se duplica la información almacenada en el vTPM, incluidas las propiedades del vTPM que el software puede utilizar para determinar la identidad de un sistema.

Cifrado y estado suspendido de máquinas virtuales de vSphere e instantáneas

A partir de vSphere 6.7, puede reanudar la operación desde una máquina virtual cifrada en estado de suspensión o revertir a una instantánea de memoria de una máquina cifrada. Puede migrar una máquina virtual cifrada con una instantánea de memoria y el estado de suspensión entre hosts ESXi.

Cifrado de máquinas virtuales de vSphere e IPv6

Puede utilizar el cifrado de máquinas virtuales de vSphere con el modo IPv6 puro o en modo mixto. Puede configurar el servidor KMS con direcciones IPv6. Puede configurar tanto vCenter Server como el KMS con solo direcciones IPv6.

Limitaciones sobre la clonación en el cifrado de máquinas virtuales de vSphere

Algunas funciones de clonación no son compatibles con el cifrado de máquinas virtuales de vSphere.

- Se admite la clonación en determinadas condiciones.
  - Se admite la clonación completa. El clon hereda el estado de cifrado del elemento principal, incluidas las claves. Puede cifrar el clon completo o volver a cifrarlo para usar claves nuevas, o descifrar el clon completo.

    Se admiten los clones vinculados y el clon hereda el estado de cifrado del elemento principal, incluidas las claves. No se puede descifrar el clon vinculado ni volver a cifrarlo con claves distintas.

    Nota Compruebe que otras aplicaciones admitan clones vinculados. Por ejemplo, VMware Horizon® 7 admite clones completos y clones instantáneos, pero no clones vinculados.
- Se admite la opción de clon instantáneo, pero no se pueden cambiar las claves de cifrado en el clon.

Configuraciones de disco no compatibles con el cifrado de máquina virtual de vSphere

No se admiten ciertos tipos de configuraciones de disco de máquina virtual con el cifrado de máquinas virtuales de vSphere.

- Asignación de dispositivos sin formato (Raw Device Mapping, RDM). Sin embargo, se admiten vSphere Virtual Volumes (vVols).
- Multiescritura o discos compartidos (MSCS, WSFC u Oracle RAC). Los archivos de "inicio" de máquina virtual cifrados son compatibles con los discos de multiescritura. Los discos virtuales cifrados no son compatibles con los discos de multiescritura. Si intenta seleccionar Multiescritura en la página **Editar configuración** de la máquina virtual con discos virtuales cifrados, se desactivará el botón **Aceptar**.

Varias limitaciones en el cifrado de máquinas virtuales de vSphere

Entre las funciones que no funcionan con el cifrado de máquinas virtuales de vSphere se encuentran las siguientes:

- vSphere Fault Tolerance
- vSphere ESXi Dump Collector
- Migración con vMotion de una máquina virtual cifrada a una instancia de vCenter Server distinta. Se admite la migración cifrada con vMotion de una máquina virtual no cifrada.
- Biblioteca de contenido
  - Las bibliotecas de contenido admiten dos tipos de plantillas, el tipo de plantilla de OVF y el tipo de plantilla de máquina virtual. No puede exportar una máquina virtual cifrada al tipo de plantilla de OVF. OVF Tool no admite máquinas virtuales cifradas. Puede crear plantillas de máquina virtual cifradas mediante el tipo de plantilla de máquina virtual. Consulte el documento *Administrar máquinas virtuales de vSphere*.
- El software para realizar copias de seguridad de discos virtuales cifrados debe utilizar VMware vSphere Storage API - Data Protection (VADP) para realizar copias de seguridad de los discos en el modo agregado en caliente o en el modo NBD con SSL habilitado. Sin embargo, no se admiten todas las soluciones de copia de seguridad que utilizan VADP para la copia de seguridad del disco virtual. Consulte con su proveedor de copias de seguridad para obtener más información.
  - Las soluciones de modo de transporte SAN de VADP no son compatibles con la copia de seguridad de discos virtuales cifrados.
  - Las soluciones de agregado en caliente de VADP son compatibles con los discos virtuales cifrados. El software de copia de seguridad debe admitir el cifrado de la máquina virtual proxy que se utiliza como parte del flujo de trabajo de copia de seguridad de agregado en caliente. El proveedor debe poseer el privilegio **Operaciones criptográficas.Cifrar máquina virtual**.

  - Las soluciones de copia de seguridad que utilizan los modos de transporte NBD-SSL son compatibles para realizar copias de seguridad de discos virtuales cifrados. La aplicación del proveedor debe poseer el privilegio **Operaciones criptográficas.Acceso directo**.

- No se pueden enviar los resultados de una máquina virtual cifrada a un puerto serie ni a un puerto paralelo. Aunque parezca que la configuración se realiza correctamente, los resultados se envían a un archivo.
- El cifrado de máquinas virtuales de vSphere no es compatible con VMware Cloud on AWS. Consulte la documentación *Administrar VMware Cloud en el centro de datos de AWS*.

Usar cifrado en el entorno de vSphere

7

Para usar cifrado en el entorno de vSphere, es necesario realizar una preparación. Una vez que el entorno está configurado, se pueden crear máquinas virtuales y discos virtuales cifrados, así como cifrar discos y máquinas virtuales existentes.

Se pueden usar la API y la CLI de `crypto-util` para realizar tareas adicionales. Consulte la *Guía de programación de vSphere Web Services SDK* para ver la documentación de API y la ayuda de la línea de comandos `crypto-util` para ver detalles de esa herramienta.

Configurar el clúster del servidor de administración de claves

Antes de comenzar con las tareas de cifrado de la máquina virtual, se debe configurar el clúster del servidor de administración de claves (KMS). Esa tarea incluye agregar el KMS y establecer confianza con el KMS. Cuando agrega un clúster, se le solicita que lo establezca como predeterminado. Se puede cambiar explícitamente el clúster predeterminado. vCenter Server aprovisiona claves del clúster predeterminado.

KMS debe ser compatible con el protocolo estándar de interoperabilidad de administración de claves (KMIP) 1.1. Consulte la *Matrices de compatibilidad de vSphere* para obtener detalles.

Puede encontrar información sobre los proveedores de KMS certificados de VMware en la Guía de compatibilidad de VMware, en la sección Plataforma y cómputo. Si selecciona las guías de compatibilidad, puede abrir la documentación de compatibilidad del servidor de administración de claves (KMS). Esta documentación se actualiza con frecuencia.

Configuración del servidor de administración de claves para cifrado de máquina virtual (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_eebiwfsy/uiConfId/49694343/)

Agregar un servidor KMS a vCenter Server en vSphere Client

Puede agregar un servidor de administración de claves (Key Management Server, KMS) al sistema de vCenter Server desde vSphere Client (cliente basado en HTML5) o mediante la API pública.

vSphere Client (cliente basado en HTML5) proporciona un asistente para agregar un KMS al sistema vCenter Server, y establecer la confianza entre KMS y vCenter Server.

vCenter Server crea un clúster de KMS cuando agrega la primera instancia de KMS.

- Después de que vCenter Server crea el clúster, puede agregar instancias de KMS del mismo proveedor al clúster.
- Puede configurar el clúster con una sola instancia de KMS.
- Si el entorno admite soluciones de KMS de diferentes proveedores, puede agregar varios clústeres de KMS.
- Si el entorno incluye varios clústeres de KMS y se elimina el clúster predeterminado, se debe establecer explícitamente otro clúster predeterminado.

Nota Los pasos siguientes se aplican a vCenter Server Appliance. Para vCenter Server en Windows, primero se le pedirá determinar que KMS confíe en vCenter Server y, a continuación, que vCenter Server confíe en KMS.

Requisitos previos

- Compruebe que el servidor de claves se encuentre en la *guía de compatibilidad de VMware para los servidores de administración de claves (Key Management Servers, KMS)*, que cumpla con KMIP 1.1, y que pueda ser un servidor y una fundición de claves simétricas.
- Compruebe que cuenta con los privilegios necesarios: **Operaciones criptográficas.Administrar servidores de claves**.
- Puede configurar el servidor KMS con direcciones IPv6.
  - Tanto vCenter Server como KMS pueden configurarse únicamente con direcciones IPv6.

Procedimiento

1 Inicie sesión en el sistema de vCenter Server con vSphere Client (cliente basado en HTML5).

2 Examine la lista de inventario y seleccione la instancia de vCenter Server.

3 Haga clic en **Configurar** y en **Servidores de administración de claves**.

4 Haga clic en **Agregar**, especifique la información de KMS en el asistente y haga clic en **Aceptar**.

5 Haga clic en **Confianza**.

   El asistente mostrará que vCenter Server confía en KMS mediante una marca de verificación verde.

6 Haga clic en **Hacer que KMS confíe en vCenter**.

7 Seleccione la opción adecuada para el servidor y complete los pasos.

Opción	Consulte
Certificado de CA raíz	Usar la opción Certificado de CA raíz para establecer una conexión de confianza.
Certificado	Usar la opción Certificado para establecer una conexión de confianza.

Opción	Consulte
Nueva solicitud de firma de certificado	Usar la opción Nueva solicitud de firma del certificado para establecer una conexión de confianza.
Cargar certificado y clave privada	Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza.

8 Haga clic en **Establecer confianza**.

El asistente mostrará que KMS confía en vCenter Server mediante una marca de verificación verde.

9 Establezca el KMS predeterminado.

a En el menú **Acciones**, seleccione **Cambiar clúster predeterminado**.

b Seleccione el clúster de KMS y haga clic en **Guardar**.

El asistente mostrará el clúster de KMS como el predeterminado actual.

Agregar un servidor KMS a vCenter Server en vSphere Web Client

Se agrega un KMS al sistema de vCenter Server desde vSphere Web Client o con la API pública.

vCenter Server crea un clúster de KMS cuando agrega la primera instancia de KMS.

- Cuando agrega el KMS, se le solicita establecer este clúster como predeterminado. Más adelante, puede cambiar explícitamente el clúster predeterminado.
- Después de que vCenter Server crea el clúster, puede agregar instancias de KMS del mismo proveedor al clúster.
- Puede configurar el clúster con una sola instancia de KMS.
- Si el entorno admite soluciones de KMS de diferentes proveedores, puede agregar varios clústeres de KMS.
- Si el entorno incluye varios clústeres de KMS y se elimina el clúster predeterminado, se debe establecer explícitamente el predeterminado. Consulte Establecer el clúster de KMS predeterminado.

Requisitos previos

- Compruebe que el servidor de claves se encuentre en *Matrices de compatibilidad de vSphere*, que cumpla con KMIP 1.1, y que pueda ser un servidor y generador de claves simétricas.
- Compruebe que cuenta con los privilegios necesarios: **Operaciones criptográficas.Administrar servidores de claves**.
- Puede configurar el servidor KMS con direcciones IPv6.
- Tanto vCenter Server como KMS pueden configurarse únicamente con direcciones IPv6.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Web Client.

2 Examine la lista de inventario y seleccione la instancia de vCenter Server.

3 Haga clic en **Configurar** y en **Servidores de administración de claves**.

4 Haga clic en **Agregar KMS**, especifique la información de KMS en el asistente y haga clic en **Aceptar**.

Opción	Valor
clúster de KMS	Seleccione **Crear nuevo clúster** para crear un nuevo clúster. Si existe un clúster, puede seleccionarlo.
Nombre del clúster	Nombre del clúster de KMS. Es posible que necesite este nombre para conectarse al KMS si la instancia de vCenter Server no está disponible.
Alias de servidor	Alias del KMS. Es posible que necesite este alias para conectarse al KMS si la instancia de vCenter Server no está disponible.
Dirección de servidor	Dirección IP o FQDN del KMS.
Puerto de servidor	Puerto en el cual vCenter Server se conecta al KMS.
Dirección de proxy	Dirección de proxy opcional para conectarse al KMS.
Puerto de proxy	Puerto de proxy opcional para conectarse al KMS.
Nombre de usuario	Algunos proveedores de KMS permiten a los usuarios especificar un nombre de usuario y una contraseña para aislar claves de cifrado utilizadas por distintos usuarios o grupos. Especifique un nombre de usuario solo si el KMS admite esta funcionalidad y si piensa utilizarla.
Contraseña	Algunos proveedores de KMS permiten a los usuarios especificar un nombre de usuario y una contraseña para aislar claves de cifrado utilizadas por distintos usuarios o grupos. Especifique una contraseña solo si el KMS admite esta funcionalidad y si piensa utilizarla.

Establecer una conexión de confianza mediante el intercambio de certificados

Después de agregar el KMS al sistema de vCenter Server, puede establecer una conexión de confianza. El proceso exacto depende de los certificados que el KMS acepte y de la directiva de la empresa.

Requisitos previos

Agregue el clúster KMS.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Haga clic en **Establecer confianza con KMS**.

5 Seleccione la opción adecuada para el servidor y complete los pasos.

Opción	Consulte
Certificado de CA raíz	Usar la opción Certificado de CA raíz para establecer una conexión de confianza.
Certificado	Usar la opción Certificado para establecer una conexión de confianza.
Nueva solicitud de firma de certificado	Usar la opción Nueva solicitud de firma del certificado para establecer una conexión de confianza.
Cargar certificado y clave privada	Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza.

Usar la opción Certificado de CA raíz para establecer una conexión de confianza

Algunos proveedores de KMS requieren que se cargue un certificado de CA raíz al KMS. Este KMS establece una conexión de confianza con todos los certificados firmados por la entidad de certificación de raíz.

El certificado de CA raíz que utiliza el cifrado de máquinas virtuales de vSphere es un certificado autofirmado que se almacena en un almacén separado en VMware Endpoint Certificate Store (VECS) en el sistema de vCenter Server.

Nota Genere un certificado de CA raíz solo si desea reemplazar los certificados existentes. En ese caso, los demás certificados que están firmados por esa entidad de certificación raíz dejan de ser válidos. Se puede generar un nuevo certificado de CA raíz como parte de este flujo de trabajo.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **Certificado de CA raíz** y haga clic en **Aceptar**.

   El cuadro de diálogo Descargar certificado de CA raíz se rellena con el certificado raíz que vCenter Server utiliza para el cifrado. Este certificado se almacena en el almacén VECS.

5 Copie el certificado en el portapapeles o descárguelo como un archivo.

6 Siga las instrucciones de su proveedor de KMS para cargar el certificado al sistema.

   Nota Algunos proveedores de KMS requieren que el proveedor de KMS reinicie el KMS para seleccionar el certificado raíz que se cargó.

Pasos siguientes

Finalice el intercambio de certificados. Consulte Completar la instalación de confianza.

Usar la opción Certificado para establecer una conexión de confianza

Algunos proveedores de KMS requieren que se cargue el certificado de vCenter Server al KMS. Después de la carga, el KMS acepta el tráfico proveniente de un sistema con ese certificado.

vCenter Server genera un certificado para proteger las conexiones con el KMS. El certificado se almacena en un almacén de claves separado en VMware Endpoint Certificate Store (VECS) en el sistema de vCenter Server.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **Certificado** y haga clic en **Aceptar**.

   El cuadro de diálogo Descargar certificado se rellena con el certificado raíz que vCenter Server utiliza para el cifrado. Este certificado se almacena en el almacén VECS.

   Nota No genere un certificado nuevo a menos que desee reemplazar los certificados existentes.

5 Copie el certificado en el portapapeles o descárguelo como un archivo.

6 Siga las instrucciones de su proveedor de KMS para cargar el certificado al KMS.

Pasos siguientes

Finalice la relación de confianza. Consulte Completar la instalación de confianza.

Usar la opción Nueva solicitud de firma del certificado para establecer una conexión de confianza

Algunos proveedores de KMS requieren que vCenter Server genere una solicitud de firma del certificado (Certificate Signing Request, CSR) y la envíe al KMS. El KMS firma la CSR y devuelve el certificado firmado. El certificado firmado se puede cargar a vCenter Server.

El uso de la opción **Nueva solicitud de firma del certificado** es un proceso de dos pasos. Primero debe generar la CSR y enviarla al proveedor de KMS. A continuación, cargue el certificado firmado que recibió del proveedor de KMS a vCenter Server.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **New Certificate Signing Request** (Nueva solicitud de firma del certificado) y haga clic en **OK** (Aceptar).

5 En el cuadro de diálogo, copie el certificado completo del cuadro de texto en el portapapeles o descárguelo como un archivo, y haga clic en **Aceptar**.

   Use el botón **Generar nueva CSR** del cuadro de diálogo únicamente si desea generar una CSR de forma explícita. Al usar esa opción, todos los certificados firmados basados en la CSR anterior dejan de ser válidos.

6 Siga las instrucciones de su proveedor de KMS para enviar la CSR.

7 Cuando reciba el certificado firmado del proveedor de KMS, vuelva a hacer clic en **Servidores de administración de claves** y vuelva a seleccionar **Nueva solicitud de firma del certificado**.

8 Pegue el certificado firmado en el cuadro de texto inferior o haga clic en **Cargar archivo** y cargue el archivo, y haga clic en **Aceptar**.

Pasos siguientes

Finalice la relación de confianza. Consulte Completar la instalación de confianza.

Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza

Algunos proveedores de KMS requieren que se carguen el certificado del servidor KMS y la clave privada al sistema vCenter Server.

Algunos proveedores de KMS generan un certificado y una clave privada para la conexión y los vuelven disponibles para el usuario. Una vez que haya cargado los archivos, el KMS establecerá una conexión de confianza con su instancia de vCenter Server.

Requisitos previos

- Solicite un certificado y una clave privada al proveedor de KMS. Los archivos son archivos X509 en formato PEM.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **Cargar certificado y clave privada** y haga clic en **Aceptar**.

5 Pegue el certificado que recibió del proveedor de KMS en el cuadro de texto superior o haga clic en **Cargar certificado** para cargar el archivo del certificado.

6 Pegue el archivo de claves en el cuadro de texto inferior o haga clic en **Cargar archivo** para cargar el archivo de claves.

7 Haga clic en **Aceptar**.

Pasos siguientes

Finalice la relación de confianza. Consulte Completar la instalación de confianza.

Establecer el clúster de KMS predeterminado

Si no establece el primer clúster como el clúster predeterminado o si el entorno usa varios clústeres y elimina el clúster predeterminado, debe establecer el clúster de KMS como predeterminado.

Requisitos previos

Como práctica recomendada, compruebe que el estado de conexión en la pestaña **Servidores de administración de claves** sea Normal y tenga una marca de verificación verde.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en la pestaña **Configurar** y en **Servidores de administración de claves** en **Más**.

3 Seleccione el clúster y haga clic en **Establecer el clúster de KMS como predeterminado**.

   No seleccione el servidor. El menú para establecer el clúster como predeterminado está disponible para ese clúster solamente.

4 Haga clic en **Yes** (Sí).

   La palabra `default` aparece junto al nombre del clúster.

Completar la instalación de confianza

A menos que el cuadro de diálogo **Agregar servidor** le haya solicitado confiar en el KMS, debe establecer la confianza explícitamente una vez finalizado el intercambio de certificados.

Es posible completar la instalación de confianza, es decir, hacer que vCenter Server confíe en el KMS, ya sea confiando en el KMS o cargando un certificado de KMS. Tiene dos opciones:

- Confiar en el certificado explícitamente por medio de la opción **Actualizar certificado de KMS**.
- Cargar un certificado de hoja de KMS o el certificado de CA de KMS en vCenter Server por medio de la opción **Cargar certificado de KMS**.

Nota Si carga el certificado de CA raíz o el certificado de CA intermedia, vCenter Server confía en todos los certificados que firma esa CA. Si desea obtener una seguridad más solida, cargue un certificado de hoja o un certificado de CA intermedia que controle el proveedor de KMS.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Para establecer la relación de confianza, actualice o cargue el certificado de KMS.

Opción	Acción
Actualizar certificado de KMS	a Haga clic en **Todas las acciones** y seleccione **Actualizar certificado de KMS**. b En el cuadro de diálogo que aparece, haga clic en **Confiar**.
Cargar certificado de KMS	a Haga clic en **Todas las acciones** y seleccione **Cargar certificado de KMS**. b En el cuadro de diálogo que aparece, haga clic en **Cargar archivo**, cargue un archivo de certificado y haga clic en **Aceptar**.

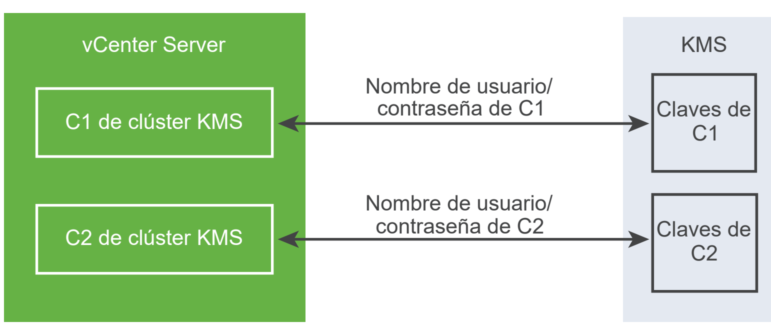
Configurar clústeres de KMS independientes para diferentes usuarios

Puede configurar su entorno con diferentes conexiones de KMS para distintos usuarios de la misma instancia de KMS. Tener varias conexiones de KMS es útil, por ejemplo, si desea conceder a distintos departamentos de su empresa acceso a diferentes conjuntos de claves del KMS.

El uso de varios clústeres de KMS permite utilizar el mismo KMS para separar las claves. Tener distintos conjuntos de claves es esencial, por ejemplo, para casos de BU o clientes diferentes.

Nota No todos los proveedores de KMS admiten varios usuarios.

Figura 7-1. Conectarse desde vCenter Server al KMS para dos usuarios distintos



Requisitos previos

Establezca la conexión con el KMS. Consulte Configurar el clúster del servidor de administración de claves.

Procedimiento

1 Cree los dos usuarios con los correspondientes nombres de usuario y contraseñas, por ejemplo, C1 y C2, en el KMS.

2 Inicie sesión en vCenter Server y cree el primer clúster de KMS.

3 Cuando se le solicite un nombre de usuario y una contraseña, proporcione información que sea exclusiva para el primer usuario.

4 Cree un segundo clúster de KMS y agregue el mismo KMS, pero utilice el segundo nombre de usuario y contraseña (C2).

Resultados

Los dos clústeres tienen conexiones independientes con el KMS y utilizan un conjunto diferente de claves.

Crear una directiva de almacenamiento de cifrado

Antes de crear máquinas virtuales cifradas, debe crear una directiva de almacenamiento de cifrado. Puede crear la directiva de almacenamiento una vez y asignarla cada vez que cifre una máquina virtual o un disco virtual.

Si desea usar el cifrado de máquinas virtuales con otros filtros de E/S, o utilizar el asistente **Crear directiva de almacenamiento de máquina virtual** en vSphere Client, consulte la documentación *Almacenamiento de vSphere* para obtener detalles.

Requisitos previos

- Establezca la conexión con el KMS.

  Si bien puede crear una directiva de almacenamiento de cifrado de máquinas virtuales sin conectarse a KMS, no es posible realizar tareas de cifrado hasta que se haya establecido una conexión de confianza con el servidor KMS.
- Privilegios necesarios: **Operaciones criptográficas.Administrar directivas de cifrado**.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Web Client.

2 Seleccione **Inicio**, haga clic en **Directivas y perfiles** y en **Directivas de almacenamiento de máquina virtual**.

3 Haga clic en **Crear directiva de almacenamiento de máquina virtual**.

4 Especifique los valores de la directiva de almacenamiento.

   a Introduzca un nombre para la directiva de almacenamiento y una descripción (opcional) y, a continuación, haga clic en **Siguiente**.

   b Si es la primera vez que usa este asistente, revise la información de **Estructura de directiva** y haga clic en **Siguiente**.

   c Seleccione la casilla **Usar reglas comunes en la directiva de almacenamiento de máquina virtual**.

   d Haga clic en **Agregar componente** y seleccione **Cifrado > Propiedades de cifrado predeterminadas**; a continuación, haga clic en **Siguiente**.

   Las propiedades predeterminadas son adecuadas en la mayoría de los casos. Necesitará una directiva personalizada únicamente si desea combinar el cifrado con otras funciones, como el almacenamiento en caché o la replicación.

   e Anule la selección de la casilla **Utilizar conjuntos de reglas en la directiva de almacenamiento** y haga clic en **Siguiente**.

f En la página **Compatibilidad de almacenamiento**, deje seleccionada la opción Compatible, elija un almacén de datos y haga clic en **Siguiente**.

g Revise la información y haga clic en **Finalizar**.

Habilitar el modo de cifrado de host de forma explícita

Es necesario habilitar el modo de cifrado de host cuando se desea ejecutar tareas de cifrado, como crear una máquina virtual cifrada, en un host ESXi. En la mayoría de los casos, el modo de cifrado de host se habilita automáticamente cuando se realiza una tarea de cifrado.

En ocasiones, es necesario activar el modo de cifrado de forma explícita. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado.

Requisitos previos

Privilegio necesario: **Operaciones criptográficas. Registrar host**

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Desplácese hasta el host ESXi y haga clic en **Configurar**.

3 En Sistema, haga clic en **Perfil de seguridad**.

4 Haga clic en **Editar** en el panel Modo de cifrado de host.

5 Seleccione **Habilitado** y haga clic en **Aceptar**.

Deshabilitar el modo de cifrado de host

El modo de cifrado de host se habilita automáticamente cuando se realiza una tarea de cifrado, si el usuario tiene privilegios suficientes para habilitar el modo de cifrado. Una vez habilitado el modo de cifrado de host, se cifran todos los volcados de núcleos para evitar la divulgación de información confidencial entre el personal de soporte. Si ya no se usa el cifrado de máquinas virtuales con un host ESXi, se puede deshabilitar el modo de cifrado.

Procedimiento

1 Elimine del registro todas las máquinas virtuales cifradas del host cuyo modo de cifrado desea deshabilitar.

2 Elimine del registro el host de vCenter Server.

3 (opcional) Si el host está en un clúster, elimine del registro los otros hosts habilitados para la encriptación de ese clúster.

4 Reinicie todos los hosts que eliminó del registro.

5 Vuelva a registrar los hosts con vCenter Server.

Resultados

El modo de cifrado de host está deshabilitado si no se agregan máquinas virtuales cifradas al host.

Crear una máquina virtual cifrada

Después de configurar KMS, es posible crear máquinas virtuales cifradas.

En esta tarea, se describe la forma de crear una máquina virtual cifrada mediante vSphere Web Client o vSphere Client (cliente basado en HTML5). vSphere Client filtra las directivas de almacenamiento para utilizar las que incluyen el cifrado de máquinas virtuales. Esto facilita la creación de máquinas virtuales cifradas.

Nota La creación de una máquina virtual cifrada demanda menos tiempo y recursos de almacenamiento que el cifrado de una máquina virtual existente. De ser posible, cifre la máquina virtual durante el proceso de creación.

Requisitos previos

- Establezca una conexión de confianza con el KMS y seleccione un KMS predeterminado.
- Cree una directiva de almacenamiento de cifrado o utilice la muestra que se incluye en el paquete (la directiva de cifrado de máquina virtual).
- Compruebe que la máquina virtual esté apagada.
- Compruebe que dispone de los privilegios requeridos:
  - **Operaciones de cifrado.Cifrar nuevo**
  - Si el modo de cifrado del host no está habilitado, también necesita **Operaciones de cifrado.Registrar host**.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client (cliente basado en HTML5) o vSphere Web Client.

2 Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Cree la máquina virtual.

   - vSphere Client: haga clic con el botón derecho en un objeto y seleccione **Nueva máquina virtual**.
   - vSphere Web Client: haga clic con el botón derecho en el objeto y seleccione **Nueva máquina virtual > Nueva máquina virtual**.

4 Siga las indicaciones para crear una máquina virtual cifrada.

Opción	Acción
Seleccionar un tipo de creación	Cree una máquina virtual nueva.
Seleccionar un nombre y una carpeta	Especifique un nombre único y una ubicación de destino para la máquina virtual.
Seleccionar un recurso informático	Especifique el objeto sobre el que tiene privilegios para crear máquinas virtuales cifradas. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado.
Seleccionar almacenamiento	vSphere Client: seleccione la casilla **Cifrar esta máquina virtual**. Se filtran las directivas de almacenamiento de máquina virtual para utilizar las que incluyen el cifrado. Seleccione una directiva de almacenamiento de máquina virtual (la muestra en el paquete es Directiva de cifrado de máquina virtual) y seleccione un almacén de datos compatible. vSphere Web Client: seleccione una directiva de almacenamiento de máquina virtual con cifrado (la muestra en el paquete es Directiva de cifrado de máquina virtual). Seleccione un almacén de datos compatible.
Seleccionar compatibilidad	Seleccione la compatibilidad. Una máquina virtual cifrada solo se puede migrar a hosts compatibles con ESXi 6.5 y de versiones posteriores.
Seleccionar un sistema operativo invitado	Seleccione el sistema operativo invitado donde planea instalar la máquina virtual posteriormente.
Personalizar hardware	Personalice el hardware, por ejemplo, cambiando el tamaño de disco o CPU. vSphere Client: (opcional) seleccione la pestaña **Opciones de máquina virtual** y abra **Cifrado**. Elija los discos que desea excluir del cifrado. Cuando se anula la selección de un disco, solo se cifran el inicio de la máquina virtual y los otros discos seleccionados. Se cifra todo disco duro nuevo que se haya agregado. Se puede cambiar la directiva de almacenamiento para discos duros individuales más tarde.
Listo para finalizar	Revise la información y haga clic en **Finalizar**.

Clonar una máquina virtual cifrada

Cuando clona una máquina virtual cifrada, el clon se cifra con las mismas claves. Para cambiar las claves del clon, desconecte la máquina virtual y repita un cifrado del clon mediante la API. Consulte *Guía de programación de vSphere Web Services SDK*.

Requisitos previos

- Establezca una conexión de confianza con el KMS y seleccione un KMS predeterminado.
- Cree una directiva de almacenamiento de cifrado o utilice la muestra que se incluye en el paquete (la directiva de cifrado de máquina virtual).
- Privilegios necesarios:
  - **Operaciones de cifrado.Clonar**

- Si el modo de cifrado del host no está habilitado, además debe tener privilegios de **Operaciones de cifrado.Registrar host**.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Para crear un clon de una máquina cifrada, haga clic con el botón derecho en la máquina virtual, seleccione **Clonar > Clonar a máquina virtual** y siga las indicaciones.

Opción	Acción
Seleccionar un nombre y una carpeta	Especifique un nombre y una ubicación de destino del clon.
Seleccionar un recurso informático	Especifique el objeto sobre el que tiene privilegios para crear máquinas virtuales cifradas. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado.
Seleccionar almacenamiento	Realice una selección en el menú **Seleccionar formato de disco virtual** y seleccione un almacén de datos. No puede cambiar la directiva de almacenamiento como parte de la operación de clonación.
Seleccionar opciones de clonación	Seleccione opciones de clonación, según lo analizado en la documentación de *Administrar máquinas virtuales de vSphere*.
Listo para finalizar	Revise la información y haga clic en **Finalizar**.

3 (opcional) Cambie las claves de la máquina virtual clonada.

De forma predeterminada, la máquina virtual clonada se crea con las mismas claves que la máquina virtual principal. Una práctica recomendada es cambiar las claves de la máquina virtual clonada para asegurarse de que varias máquinas virtuales no tengan las mismas claves.

a Apague la máquina virtual.

b Repita el cifrado del clon mediante la API. Consulte *Guía de programación de vSphere Web Services SDK*.

Para usar otros DEK y KEK, repita un cifrado profundo de la máquina virtual clonada. Para usar otro KEK, repita un cifrado superficial de la máquina virtual clonada. Puede realizar una operación de repetición de cifrado superficial mientras la máquina virtual se encuentra encendida, a menos que la máquina virtual contenga instantáneas.

Cifrar una máquina virtual o un disco virtual existente

Es posible cifrar una máquina virtual o un disco virtual existente si se cambia su directiva de almacenamiento. Solo se pueden cifrar discos virtuales de máquinas virtuales cifradas.

En esta tarea, se describe la forma de cifrar una máquina virtual o un disco virtual existente mediante vSphere Client (cliente basado en HTML5) o vSphere Web Client.

Cifrar máquinas virtuales con vSphere Client (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_cehw9rah/uiConfId/49694343/)

Requisitos previos

- Establezca una conexión de confianza con el KMS y seleccione un KMS predeterminado.
- Cree una directiva de almacenamiento de cifrado o utilice la muestra que se incluye en el paquete (la directiva de cifrado de máquina virtual).
- Compruebe que la máquina virtual esté apagada.
- Compruebe que dispone de los privilegios requeridos:
  - **Operaciones de cifrado.Cifrar nuevo**
  - Si el modo de cifrado del host no está habilitado, también necesita **Operaciones de cifrado.Registrar host**.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client (cliente basado en HTML5) o vSphere Web Client.

2 Haga clic con el botón derecho en la máquina virtual que desea modificar y seleccione **Directivas de máquina virtual > Editar directivas de almacenamiento de máquina virtual**.

   Es posible establecer la directiva de almacenamiento para los archivos de la máquina virtual, que se representan con Inicio de la máquina virtual, y la directiva de almacenamiento para los discos virtuales.

3 Seleccione la directiva de almacenamiento.

   - vSphere Client (cliente basado en HTML5):
     - Para cifrar la máquina virtual y sus discos duros, seleccione una directiva de almacenamiento de cifrado y haga clic en **Aceptar**.
     - Para cifrar la máquina virtual, pero no los discos virtuales, active **Configurar por disco**, seleccione la directiva de almacenamiento de cifrado para Inicio de la máquina virtual y otras directivas de almacenamiento para los discos virtuales, y haga clic en **Aceptar**.
   - vSphere Web Client:
     - Para cifrar la máquina virtual y sus discos duros, seleccione una directiva de almacenamiento de cifrado y haga clic en **Aplicar a todo**.
     - Para cifrar la máquina virtual, pero no los discos virtuales, seleccione la directiva de almacenamiento de cifrado para Inicio de la máquina virtual y otras directivas de almacenamiento para los discos virtuales, y haga clic en **Aplicar**.

   No se puede cifrar el disco virtual de una máquina virtual sin cifrar.

4 Si lo prefiere, puede cifrar la máquina virtual, o la máquina virtual y los discos, en el menú **Editar configuración** de vSphere Client.

   a Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

   b Seleccione la pestaña **Opciones de máquina virtual** y abra **Cifrado**. Elija una directiva de cifrado. Si anula la selección de todos los discos, solo se cifrará el inicio de la máquina virtual.

   c Haga clic en **Aceptar**.

Descifrar una máquina virtual o un disco virtual cifrados

Puede descifrar una máquina virtual, sus discos o ambos si cambia la directiva de almacenamiento.

En esta tarea, se describe la forma de descifrar una máquina virtual cifrada mediante vSphere Client (cliente basado en HTML5) o vSphere Web Client.

Todas las máquinas virtuales cifradas requieren vMotion cifrado. Durante el descifrado de la máquina virtual, se conserva la configuración de vMotion cifrado. Para cambiar esta opción y dejar de usar vMotion cifrado, cambie de forma explícita la configuración.

En esta tarea se explica la forma de ejecutar el descifrado mediante las directivas de almacenamiento. En los discos virtuales, se puede realizar el descifrado mediante el menú **Editar configuración**.

Requisitos previos

- La máquina virtual debe estar cifrada.
- La máquina virtual debe estar apagada o en modo de mantenimiento.
- Privilegios necesarios: **Operaciones criptográficas.Descifrar**

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client (cliente basado en HTML5) o vSphere Web Client.

2 Haga clic con el botón derecho en la máquina virtual que desea modificar y seleccione **Directivas de máquina virtual > Editar directivas de almacenamiento de máquina virtual**.

   Es posible establecer la directiva de almacenamiento para los archivos de la máquina virtual, que se representan con Inicio de la máquina virtual, y la directiva de almacenamiento para los discos virtuales.

3 Seleccione una directiva de almacenamiento.

   - vSphere Client (cliente basado en HTML5):
     - Para descifrar la máquina virtual y sus discos duros, desactive **Configurar por disco**, seleccione una directiva de almacenamiento en el menú desplegable y haga clic en **Aceptar**.

  - Para descifrar un disco virtual, pero no la máquina virtual, active **Configurar por disco**, seleccione la directiva de almacenamiento de cifrado para Inicio de la máquina virtual y otras directivas de almacenamiento correspondientes a los discos virtuales, y haga clic en **Aceptar**.

- vSphere Web Client:

  - Para descifrar la máquina virtual y sus discos duros, seleccione una directiva de almacenamiento en el menú desplegable, haga clic en **Aplicar a todo** y en **Aceptar**.

  - Para descifrar un disco virtual, pero no la máquina virtual, seleccione una directiva de almacenamiento para el disco virtual en el menú desplegable de la tabla. No cambie la directiva para Inicio de la máquina virtual. Haga clic en **Aceptar**.

No se puede descifrar la máquina virtual y dejar el disco cifrado.

4 Si lo prefiere, puede usar vSphere Client (cliente basado en HTML5) para descifrar la máquina virtual y los discos en el menú **Editar configuración**.

a Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

b Seleccione la pestaña **Opciones de máquina virtual** y expanda **Cifrado**.

c Para descifrar la máquina virtual y sus discos duros, elija **Ninguno** en el menú desplegable **Cifrar máquina virtual**.

d Para descifrar un disco virtual, pero no la máquina virtual, anule la selección del disco.

e Haga clic en **Aceptar**.

5 (opcional) Puede modificar la opción de configuración vMotion cifrado.

a Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

b Haga clic en **Opciones de máquina virtual** y abra **Cifrado**.

c Establezca el valor de **vMotion cifrado**.

Cambiar la directiva de cifrado para discos virtuales

Cuando crea una máquina virtual cifrada desde vSphere Web Client, todos los discos virtuales que agrega durante la creación de la máquina virtual están cifrados. Puede descifrar discos virtuales que están cifrados con la opción **Editar directivas de almacenamiento de máquina virtual**.

Nota Una máquina virtual cifrada puede tener discos virtuales que no estén cifrados. Sin embargo, una máquina virtual no cifrada no puede tener discos virtuales cifrados.

Consulte Cifrado de disco virtual.

En esta tarea, se describe la forma de cambiar la directiva de cifrado mediante directivas de almacenamiento. Puede utilizar vSphere Client (cliente basado en HTML5) o vSphere Web Client. También puede usar el menú **Editar configuración** para realizar este cambio.

Requisitos previos

- Debe tener el privilegio **Operaciones criptográficas.Administrar directivas de cifrado**.
- Compruebe que la máquina virtual esté apagada.

Procedimiento

1. Conéctese a vCenter Server mediante vSphere Client (cliente basado en HTML5) o vSphere Web Client.
2. Haga clic con el botón derecho en la máquina virtual y seleccione **Directivas de máquina virtual > Editar directivas de almacenamiento de máquina virtual**.
3. Cambie la directiva de almacenamiento.
   - vSphere Client (cliente basado en HTML5):
     - Para cambiar la directiva de almacenamiento de la máquina virtual y sus discos duros, seleccione una directiva de almacenamiento de cifrado y haga clic en **Aceptar**.
     - Para cifrar la máquina virtual, pero no los discos virtuales, active **Configurar por disco**, seleccione la directiva de almacenamiento de cifrado para Inicio de la máquina virtual y otras directivas de almacenamiento para los discos virtuales, y haga clic en **Aceptar**.
   - vSphere Web Client:
     - Para cambiar la directiva de almacenamiento de la máquina virtual y sus discos duros, seleccione una directiva de almacenamiento de cifrado y haga clic en **Aplicar a todo**.
     - Para cifrar la máquina virtual, pero no los discos virtuales, seleccione la directiva de almacenamiento de cifrado para Inicio de la máquina virtual y otras directivas de almacenamiento para los discos virtuales, y haga clic en **Aplicar**.

   No se puede cifrar el disco virtual de una máquina virtual sin cifrar.
4. Si lo prefiere, puede cambiar la directiva de almacenamiento desde el menú **Editar configuración**.
   a. Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.
   b. Seleccione la pestaña **Hardware virtual**, expanda un disco duro y elija una directiva de cifrado en el menú desplegable.
   c. Haga clic en **Aceptar**.

Resolver problemas de claves faltantes

En ciertas circunstancias, el host ESXi no puede obtener la clave (KEK) para una máquina virtual cifrada o un disco virtual cifrado desde vCenter Server. En ese caso, todavía puede cancelar el registro o volver a cargar la máquina virtual. Sin embargo, no puede realizar otras operaciones con la máquina virtual, como encenderla o eliminarla. Una alarma de vCenter Server notifica cuando una máquina virtual cifrada se encuentra en estado bloqueado. Para desbloquear una

máquina virtual cifrada bloqueada, puede usar vSphere Client después de realizar los pasos necesarios a fin de que las claves requeridas estén disponibles en el KMS.

Si la clave de la máquina virtual no está disponible, el estado de la máquina virtual se muestra como no válido. No se puede encender la máquina virtual. Si la clave de la máquina virtual está disponible, pero no hay disponible una clave para un disco cifrado, el estado de la máquina virtual no se muestra como no válido. Sin embargo, la máquina virtual no se puede encender y aparece el siguiente error:

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

Nota El siguiente procedimiento muestra las situaciones que pueden causar el bloqueo de una máquina virtual, las alarmas y los registros de eventos correspondientes que aparecen y lo que se debe hacer en cada caso.

Procedimiento

1 Si el problema es la conexión entre el sistema de vCenter Server y el KMS, se genera una alarma de máquina virtual y aparece el siguiente mensaje en el registro de eventos:

   `La máquina virtual está bloqueada debido a un error del clúster de KMS.`

   Manualmente, debe comprobar las claves en el clúster de KMS y restaurar la conexión con el clúster de KMS. Cuando el KMS y las claves vuelvan a estar disponibles, desbloquee las máquinas virtuales bloqueadas. Consulte Desbloquear las máquinas virtuales bloqueadas. También puede reiniciar el host y volver a registrar la máquina virtual para desbloquearla después de restaurar la conexión.

   Al perder la conexión con el KMS, la máquina virtual no se bloquea automáticamente. La máquina virtual solo entra en un estado bloqueado si se cumplen las siguientes condiciones:

   - La clave no está disponible en el host ESXi.
   - vCenter Server no puede recuperar las claves del KMS.

   Después de cada reinicio, un host ESXi debe poder acceder a vCenter Server. vCenter Server solicita la clave con el identificador correspondiente del KMS y la pone a disposición de ESXi.

   Si después de restaurar la conexión con el clúster de KMS, la máquina virtual permanece bloqueada, consulte Desbloquear las máquinas virtuales bloqueadas.

2 Si se restaura la conexión, registre la máquina virtual. Si se produce un error al intentar registrar la máquina virtual, compruebe que tiene el privilegio **Operaciones criptográficas.Registrar máquina virtual** para el sistema de vCenter Server.

   Este privilegio no es necesario para encender una máquina virtual cifrada si la clave está disponible. No obstante, sí es necesario para registrar la máquina virtual si la clave debe recuperarse.

3 Si la clave ya no está disponible en el KMS, se genera una alarma en la máquina virtual y aparece el siguiente mensaje en el registro de eventos:

`La máquina virtual está bloqueada porque faltan claves en el clúster de KMS.`

Solicite al administrador de KMS que restaure la clave. Puede encontrar una clave inactiva si va a encender una máquina virtual que se había quitado del inventario y no se había registrado por un largo período. También sucede si reinicia el host ESXi y el KMS no está disponible.

   a Recupere el identificador de clave mediante el explorador de objetos administrados (Managed Object Browser, MOB) o vSphere API.

      Recupere el valor de `keyId` de `VirtualMachine.config.keyId.keyId`.

   b Solicite al administrador de KMS que reactive la clave que está asociada con ese identificador de clave.

   c Tras restaurar la clave, consulte Desbloquear las máquinas virtuales bloqueadas.

Si la clave se puede restaurar en el KMS, vCenter Server la recupera y la envía al host ESXi la próxima vez que se la necesita.

4 Si se puede acceder al KMS y el host ESXi está encendido, pero el sistema vCenter Server no está disponible, siga estos pasos para desbloquear las máquinas virtuales.

   a Restaure el sistema de vCenter Server o configure un sistema de vCenter Server diferente y, a continuación, establezca confianza con KMS.

      Debe usar el mismo nombre de clúster de KMS, pero la dirección IP de KMS puede ser diferente.

   b Vuelva a registrar todas las máquinas virtuales que están bloqueadas.

      La nueva instancia de vCenter Server recupera las claves del KMS y las máquinas virtuales se desbloquean.

5 Si faltan las claves solo en el host ESXi, se genera una alarma de máquina virtual y aparece el siguiente mensaje en el registro de eventos:

`La máquina virtual está bloqueada porque faltan claves en el host.`

El sistema de vCenter Server puede recuperar las claves que faltan desde el clúster de KMS. No se requiere la recuperación manual de las claves. Consulte Desbloquear las máquinas virtuales bloqueadas.

Desbloquear las máquinas virtuales bloqueadas

Una alarma de vCenter Server notifica cuando una máquina virtual cifrada se encuentra en estado bloqueado. Para desbloquear una máquina virtual cifrada bloqueada, puede usar vSphere Client (cliente basado en HTML5) después de seguir los pasos necesarios para que las claves requeridas estén disponibles en el KMS.

Requisitos previos

- Compruebe que cuenta con los privilegios necesarios: **Operaciones criptográficas.RegisterVM**.
- Podrían ser necesarios otros privilegios para realizar tareas opcionales, como habilitar el cifrado de host.
- Antes de desbloquear una máquina virtual bloqueada, resuelva la causa del bloqueo e intente solucionar el problema manualmente. Consulte Resolver problemas de claves faltantes.

Procedimiento

1. Conéctese a vCenter Server mediante vSphere Client.
2. Desplácese hasta la pestaña **Resumen** de la máquina virtual.

   Cuando una máquina virtual está bloqueada, aparece la alarma de máquina virtual bloqueada.
3. Decida si quiere confirmar la alarma o restablecerla en verde, pero sin desbloquear ahora la máquina virtual.

   Al hacer clic en **Confirmar** o **Restablecer a verde**, la alarma desaparece, pero la máquina virtual permanecerá bloqueada hasta que la desbloquee.
4. Desplácese hasta la pestaña **Supervisar** de la máquina virtual y haga clic en **Eventos** para obtener más información sobre el motivo por el cual la máquina virtual está bloqueada.
5. Antes de desbloquear la máquina virtual, solucione los problemas según lo sugerido.
6. Desplácese hasta la pestaña de **Resumen** de la máquina virtual y haga clic en **Desbloquear máquina virtual**, debajo de la consola de máquina virtual.

   Se muestra un mensaje para advertir que los datos de claves de cifrado se transmitirán al host.
7. Haga clic en **Sí**.

Solucionar problemas del modo de cifrado de host ESXi

En ciertas circunstancias, el modo de cifrado de host ESXi puede deshabilitarse.

Un host ESXi requiere que esté habilitado el modo de cifrado de ese host si contiene máquinas virtuales cifradas. Si el host detecta que falta su clave de host o si el clúster de KMS no está disponible, es posible que el host no logre habilitar el modo de cifrado. vCenter Server genera una alarma cuando no se puede habilitar el modo de cifrado de host.

Procedimiento

1. Si el problema es la conexión entre el sistema de vCenter Server y el clúster de KMS, se genera una alarma y aparece un mensaje de error en el registro de eventos.

   Debe restaurar la conexión con el clúster de KMS que contiene las claves de cifrado en cuestión.

2 Si faltan claves, se genera una alarma y aparece un mensaje de error en el registro de eventos.

   Debe asegurarse de que las claves estén presentes en el clúster de KMS. Consulte la documentación del proveedor de administración de claves para obtener información sobre cómo restaurar a partir de una copia de seguridad.

Pasos siguientes

Si el modo de cifrado del host permanece deshabilitado después de restaurar la conexión con el clúster de KMS o de recuperar manualmente las claves para el clúster de KMS, vuelva a habilitar el modo de cifrado de host. Consulte Volver a habilitar el modo de cifrado de host ESXi.

Volver a habilitar el modo de cifrado de host ESXi

A partir de vSphere 6.7, una alarma de vCenter Server notifica cuando el modo de cifrado de host ESXi se deshabilita. En vSphere 6.7, se puede volver a habilitar el modo de cifrado de host.

Requisitos previos

- Compruebe que cuenta con los privilegios necesarios: **Operaciones criptográficas.Registrar host**.
- Antes de volver a habilitar el modo de cifrado, investigue la causa e intente solucionar el problema manualmente.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Desplácese hasta la pestaña **Resumen** del host ESXi.

   Cuando se deshabilita el modo de cifrado, se muestra la alarma El host requiere el modo de cifrado habilitado.

3 Decida si quiere confirmar la alarma o restablecerla a verde, pero sin volver a habilitar el modo de cifrado de host ahora.

   Al hacer clic en **Confirmar** o **Restablecer a verde**, la alarma desaparece, pero el modo de cifrado de host permanece deshabilitado hasta que vuelva a habilitarlo.

4 Desplácese hacia la pestaña **Supervisar** del host ESXi y haga clic en **Eventos** para obtener más información sobre el motivo por el que se deshabilitó el modo de cifrado.

   Solucione los problemas sugeridos antes de volver a habilitar el modo de cifrado.

5 En la pestaña **Resumen**, haga clic en **Habilitar el modo de cifrado de host** para volver a habilitar el cifrado de host.

   Se muestra un mensaje para advertir que los datos de claves de cifrado se transmitirán al host.

6 Haga clic en **Sí**.

Establecer el umbral de caducidad de los certificados del servidor de administración de claves

De forma predeterminada, vCenter Server envía una notificación 30 días antes de que caduquen los certificados del servidor de administración de claves (Key Management Server, KMS). Puede cambiar este valor predeterminado.

Los certificados de KMS tienen fecha de caducidad. Recibirá una alerta cuando se alcance el umbral de la fecha de caducidad.

vCenter Server y los clústeres de KMS intercambian dos tipos de certificados: servidor y cliente. La instancia de VMware Endpoint Certificate Store (VECS) del sistema de vCenter Server almacena los certificados del servidor y un certificado de cliente por cada clúster de KMS. Debido a que existen dos tipos de certificados, hay dos alarmas para cada tipo de certificado (una para el cliente y una para el servidor).

Procedimiento

1 Inicie sesión en un sistema vCenter Server mediante vSphere Client.
2 Seleccione el sistema de vCenter Server en la jerarquía de objetos.
3 Haga clic en **Configurar**.
4 En **Configuración**, haga clic en **Configuración avanzada** y, a continuación, en **Editar configuración**.
5 Haga clic en el icono **Filtrar** e introduzca `vpxd.kmscert.threshold`, o bien desplácese hasta el propio parámetro de configuración.
6 Escriba el valor en días y haga clic en **Guardar**.

Cifrado de máquinas virtuales de vSphere y volcados de núcleo

Si el entorno utiliza cifrado de máquinas virtuales de vSphere y si se produce un error en el host ESXi, el volcado de núcleo resultante se cifra para proteger los datos del cliente. Los volcados de núcleo que se incluyen en el paquete de vm-support también están cifrados.

Nota Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad de datos y privacidad de la organización al gestionar el volcado de núcleo.

Volcados de núcleo en hosts ESXi

Cuando un host ESXi, el ámbito de un usuario o una máquina virtual se bloquean, se genera un volcado de núcleo y se reinicia el host. Si el host ESXi tiene habilitado el modo de cifrado, el volcado de núcleo se cifra con una clave que se encuentra en la memoria caché de claves de ESXi. Esta clave viene del KMS. Consulte Cómo el cifrado de máquinas virtuales de vSphere protege el entorno para obtener información general.

En la siguiente tabla, se muestran las claves de cifrado que se utilizan para cada tipo de volcado de núcleo, según la versión de vSphere.

Tabla 7-1. Claves de cifrado de volcado de núcleo

Tipo de volcado de núcleo	Clave de cifrado (ESXi 6.5)	Clave de cifrado (ESXi 6.7 y versiones posteriores)
Kernel de ESXi	Clave de host	Clave de host
Ámbito del usuario (hostd)	Clave de host	Clave de host
Máquina virtual cifrada	Clave de host	Clave de la máquina virtual

Las acciones que puede realizar después de un reinicio del host ESXi dependen de varios factores.

- En la mayoría de los casos, vCenter Server recupera la clave del host del KMS e intenta insertar la clave en el host ESXi después de reiniciar. Si la operación se realiza correctamente, se puede generar el paquete de vm-support y descifrar el volcado de núcleo, o bien volver a cifrarlo. Consulte Descifrar o volver a cifrar un volcado de núcleo cifrado.
- Si vCenter Server no puede conectarse al host ESXi, tal vez pueda recuperar la clave del KMS. Consulte Resolver problemas de claves faltantes.
- Si el host usó una clave personalizada que no es igual a la clave que vCenter Server inserta en el host, no podrá manipular el volcado de núcleo. Evite usar claves personalizadas.

Volcados de núcleo y paquetes de vm-support

Si se comunica con el soporte técnico de VMware debido a un error grave, el representante de soporte, por lo general, le pedirá que genere un paquete de vm-support. El paquete incluye archivos de registro y otra información, incluso volcados de núcleo. Si los representantes de soporte no pueden resolver los inconvenientes al analizar los archivos de registro y otra información, tal vez le soliciten que descifre los volcados de núcleo y que habilite la información relevante. Para proteger información confidencial, como las claves, siga la directiva de privacidad y seguridad de su organización. Consulte Recopilar un paquete de vm-support para un host ESXi que usa cifrado.

Volcados de núcleo de sistemas de vCenter Server

Un volcado de núcleo de un sistema de vCenter Server no está cifrado. vCenter Server ya contiene información posiblemente confidencial. Como mínimo, asegúrese de que el sistema Windows donde se ejecuta vCenter Server Appliance o vCenter Server estén protegidos. Consulte Capítulo 4 Proteger sistemas vCenter Server. Asimismo, también se recomienda apagar los volcados de núcleo del sistema de vCenter Server. Otra información de los archivos de registro puede ayudar a determinar el problema.

Recopilar un paquete de vm-support para un host ESXi que usa cifrado

Si se habilita el modo de cifrado de hosts para el host ESXi, se cifran los volcados de núcleo presentes en el paquete de `vm-support`. Puede recopilar el paquete desde vSphere Client y especificar una contraseña si piensa descifrar el volcado de núcleo más adelante.

El paquete de `vm-support` incluye archivos de registro, archivos de volcado de núcleo, entre otros.

Requisitos previos

Informe a su representante de soporte si se habilita el modo de cifrado para el host ESXi.
Es posible que el representante le pida descifrar los volcados de núcleo y extraer información relevante.

Nota Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad y privacidad de la organización para proteger información confidencial, como claves de host.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Client.

2 Haga clic en **Hosts y clústeres**, y haga clic con el botón secundario en el host ESXi.

3 Seleccione **Exportar registros del sistema**.

4 En el cuadro de diálogo, seleccione **Contraseña para volcados de núcleo cifrados** y, a continuación, especifique y confirme una contraseña.

5 Deje los valores predeterminados para las otras opciones o realice cambios si así lo requiere el soporte técnico de VMware, y haga clic en **Exportar registros**.

6 Especifique una ubicación para el archivo.

7 Si su representante de soporte le pidió descifrar el volcado de núcleo en el paquete de `vm-support`, inicie sesión en cualquier host ESXi y siga estos pasos.

   a Inicie sesión en ESXi y conéctese al directorio donde está ubicado el paquete de `vm-support`.

      El nombre de archivo sigue el patrón esx.fecha_hora.tgz.

   b Asegúrese de que el directorio tenga suficiente espacio para el paquete, el paquete descomprimido y el paquete nuevamente comprimido; o bien mueva el paquete.

c Extraiga el paquete en el directorio local.

```
vm-support -x *.tgz .
```

La jerarquía de archivos resultante puede contener los archivos de volcado de núcleo del host ESXi, generalmente en `/var/core`, y puede contener varios archivos de volcado de núcleo de las máquinas virtuales.

d Descifre cada archivo de volcado de núcleo cifrado por separado.

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

vm-support-incident-key-file es el archivo de clave del incidente que se encuentra en el nivel superior del directorio.

encryptedZdump es el nombre del archivo de volcado de núcleo cifrado.

decryptedZdump es el nombre del archivo que genera el comando. Procure que el nombre sea similar al nombre de *encryptedZdump*.

e Proporcione la contraseña que especificó al crear el paquete de `vm-support`.

f Elimine los volcados de núcleo cifrados y vuelva a comprimir el paquete.

```
vm-support --reconstruct
```

8 Elimine los archivos que contienen información confidencial.

Resultados

Exportar paquetes de soporte de host con contraseñas (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_xum9fnl1/uiConfId/49694343/)

Descifrar o volver a cifrar un volcado de núcleo cifrado

Para descifrar o volver a cifrar un volcado de núcleo cifrado en el host ESXi, puede usar la CLI `crypto-util`.

Puede descifrar y examinar por su cuenta los volcados de núcleo en el paquete de vm-support. Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad y privacidad de la organización para proteger la información confidencial como las claves.

Para obtener detalles sobre cómo volver a cifrar un volcado de núcleo y sobre otras funciones de `crypto-util`, consulte la ayuda de la línea de comandos.

Nota `crypto-util` es para usuarios avanzados.

Requisitos previos

La clave que se usó para cifrar el volcado de núcleo debe estar disponible en el host ESXi que generó el volcado de núcleo.

Procedimiento

1 Inicie sesión directamente en el host ESXi en donde se produjo el volcado de núcleo.

  Si el host ESXi se encuentra en el modo de bloqueo, o si el acceso SSH está deshabilitado, es posible que deba habilitar el acceso en primer lugar.

2 Determine si el volcado de núcleo está cifrado.

Opción	Descripción
Supervisar el volcado de núcleo	`crypto-util envelope describe vmmcores.ve`
archivo zdump	`crypto-util envelope describe --offset 4096` *`zdumpFile`*

3 Descifre el volcado de núcleo según su tipo.

Opción	Descripción
Supervisar el volcado de núcleo	`crypto-util envelope extract vmmcores.ve vmmcores`
archivo zdump	`crypto-util envelope extract --offset 4096` *`zdumpEncrypted zdumpUnencrypted`*

Proteger las máquinas virtuales con el módulo de plataforma de confianza virtual

8

Con la función Módulo de plataforma de confianza virtual (vTPM), puede agregar un procesador criptográfico virtual de TPM 2.0 a una máquina virtual.

Un vTPM es una representación basada en software de un chip de módulo de plataforma de confianza 2.0 físico. Un vTPM actúa como cualquier otro dispositivo virtual. Puede agregar un vTPM a una máquina virtual de la misma manera que agrega memoria, controladoras de disco, controladoras de red o CPU virtuales. Un vTPM no requiere un chip de módulo de plataforma de confianza de hardware.

Este capítulo incluye los siguientes temas:

- Descripción general del módulo de plataforma de confianza virtual
- Crear una máquina virtual con un módulo de plataforma de confianza virtual
- Habilitar el Módulo de plataforma de confianza virtual para una máquina virtual existente
- Quitar el módulo de plataforma de confianza virtual de una máquina virtual
- Identificar las máquinas virtuales habilitadas para el módulo de la plataforma de confianza virtual
- Ver certificados de dispositivo del módulo de plataforma de confianza virtual
- Exportar y reemplazar certificados de dispositivo del Módulo de plataforma de confianza

Descripción general del módulo de plataforma de confianza virtual

Un módulo de plataforma de confianza virtual (virtual Trusted Platform Module, vTPM) es una representación basada en software de un chip de módulo de plataforma de confianza 2.0 físico. Un vTPM actúa como cualquier otro dispositivo virtual.

Introducción a los vTPM

Los vTPM proporcionan funciones basadas en hardware relacionadas con la seguridad, como la generación aleatoria de números, la atestación y la generación de claves, entre otras. Cuando se agrega un vTPM a una máquina virtual, permite que el sistema operativo invitado cree y almacene claves que son privadas. Estas claves no están expuestas al sistema operativo invitado en sí. Por lo

tanto, se reduce la superficie de ataque de la máquina virtual. Por lo general, al poner en peligro el sistema operativo invitado, se compromete su información confidencial, pero la habilitación de un vTPM reduce este riesgo en gran medida. Estas claves solo las puede utilizar el sistema operativo invitado para fines de cifrado o firma. Con un vTPM asociado, un tercero puede dar fe (validar) remotamente de la identidad del firmware y del sistema operativo invitado.

Se puede agregar un vTPM a una máquina virtual nueva o existente. Un vTPM depende del cifrado de máquinas virtuales para proteger los datos esenciales del TPM. Al configurar un vTPM, se cifran los archivos de la máquina virtual, pero no los discos. Puede optar por agregar cifrado de forma explícita para la máquina virtual y sus discos.

Cuando se hace una copia de seguridad de una máquina virtual habilitada con un vTPM, la copia de seguridad debe incluir todos los datos de la máquina virtual, incluido el archivo `*.nvram`. Si la copia de seguridad no incluye el archivo `*.nvram`, no se puede restaurar una máquina virtual con un vTPM. Asimismo, debido a que los archivos de inicio de una máquina virtual con un vTPM habilitado están cifrados, asegúrese de que las claves de cifrado estén disponibles en el momento de la restauración.

El vTPM no requiere un chip físico de TPM 2.0 presente en el host ESXi. No obstante, si desea realizar la atestación de host, es necesaria una entidad externa, como un chip físico de TPM 2.0. Consulte Proteger hosts ESXi con el módulo de plataforma de confianza.

Nota De manera predeterminada, no hay ninguna directiva de almacenamiento asociada a una máquina virtual habilitada con un vTPM. Solo están cifrados los archivos de máquina virtual (Inicio de la máquina virtual). Si lo prefiere, puede agregar cifrado de forma explícita para la máquina virtual y sus discos, pero los archivos de máquina virtual ya se habrán cifrado.

Requisitos para vTPM

Para utilizar un vTPM, el entorno de vSphere debe cumplir con estos requisitos:

- Requisitos de la máquina virtual:
  - Firmware EFI.
  - Versión de hardware 14 o posterior
- Requisitos de los componentes:
  - vCenter Server 6.7 o una versión posterior para máquinas virtuales Windows.
  - Cifrado de máquinas virtuales (para cifrar los archivos de inicio de la máquina virtual).
  - Proveedor de claves configurado para vCenter Server. Consulte Configurar el clúster del servidor de administración de claves.
- Compatibilidad con el sistema operativo invitado:
  - Windows Server 2008 y versiones posteriores
  - Windows 7 y versiones posteriores

Diferencias entre un TPM de hardware y un TPM virtual

Un módulo de plataforma de confianza (Trusted Platform Module, TPM) de hardware se usa para proporcionar un almacenamiento de credenciales o claves seguro. Un vTPM realiza las mismas funciones que un TPM, pero lleva a cabo las capacidades de coprocesador cifrado en un software. El vTPM utiliza el archivo `.nvram`, que se cifra mediante el cifrado de máquinas virtuales, a modo de almacenamiento seguro.

El TPM de hardware incluye una clave precargada denominada “clave de aprobación” (Endorsement Key, EK). La EK está formada por una clave pública y una privada. La EK proporciona al TPM una identidad exclusiva. Esta clave se proporciona para un vTPM mediante VMware Certificate Authority (VMCA) o una entidad de certificación (Certificate Authority, CA) de terceros. Una vez que el vTPM utiliza una clave, por lo general, no se la cambia debido a que se invalidaría la información confidencial almacenada en el vTPM. El vTPM no se comunica con la CA externa en ningún momento.

Crear una máquina virtual con un módulo de plataforma de confianza virtual

Puede agregar un módulo de plataforma de confianza virtual (vTPM) a una máquina virtual para proporcionar mayor seguridad al sistema operativo invitado. Antes de poder agregar un vTPM, se debe configurar el KMS.

Puede habilitar vTPM para las máquinas virtuales que se ejecutan en vSphere 6.7 y versiones posteriores. El TPM virtual de VMware es compatible con TPM 2.0 y crea un chip virtual habilitado para TPM para que lo empleen la máquina virtual y el sistema operativo invitado que aloja.

Requisitos previos

- Asegúrese de que el entorno de vSphere está configurado para el cifrado de la máquina virtual. Consulte Configurar el clúster del servidor de administración de claves.
- El sistema operativo invitado que utilice puede ser Windows Server 2008 y versiones posteriores y Windows 7 y versiones posteriores.
- Los hosts ESXi que se ejecuten en el entorno deben ser ESXi 6.7 o una versión posterior.
- La máquina virtual debe usar firmware EFI.
- Compruebe que dispone de los privilegios requeridos:
  - **Operaciones de cifrado.Clonar**
  - **Operaciones de cifrado.Cifrar**
  - **Operaciones de cifrado.Cifrar nuevo**
  - **Operaciones de cifrado.Registrar máquina virtual**

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Haga clic con el botón derecho en el objeto, seleccione **Nueva máquina virtual** y siga las indicaciones para crear una máquina virtual.

Opción	Acción
Seleccionar un tipo de creación	Cree una máquina virtual nueva.
Seleccionar un nombre y una carpeta	Especifique un nombre y una ubicación de destino.
Seleccionar un recurso informático	Especifique el objeto sobre el que tiene privilegios para crear máquinas virtuales. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado.
Seleccionar almacenamiento	Seleccione un almacén de datos compatible.
Seleccionar compatibilidad	Seleccione **ESXi 6.7 y versiones posteriores**.
Seleccionar un sistema operativo invitado	Seleccione Windows Server 2016 (64 bits) o Windows 10 (64 bits) para su uso como sistema operativo invitado.
Personalizar hardware	Haga clic en **Agregar nuevo dispositivo** y seleccione **Módulo de plataforma de confianza**. Puede personalizar aún más el hardware, por ejemplo, cambiando el tamaño del disco o la CPU.
Listo para finalizar	Revise la información y haga clic en **Finalizar**.

Resultados

La máquina virtual que admite vTPM aparece en el inventario según lo especificado.

Habilitar el Módulo de plataforma de confianza virtual para una máquina virtual existente

Puede agregar un módulo de plataforma de confianza virtual (vTPM) a una máquina virtual existente para proporcionar una mayor seguridad al sistema operativo invitado. Antes de poder agregar un vTPM, se debe configurar el KMS.

Puede habilitar vTPM para las máquinas virtuales que se ejecutan en vSphere 6.7 y versiones posteriores. El TPM virtual de VMware es compatible con TPM 2.0 y crea un chip virtual que admite TPM para usarlo con la máquina virtual y el sistema operativo invitado que aloja.

Requisitos previos

- Asegúrese de que el entorno de vSphere está configurado para el cifrado de la máquina virtual. Consulte Configurar el clúster del servidor de administración de claves.
- El sistema operativo invitado que utilice puede ser Windows Server 2008 y versiones posteriores y Windows 7 y versiones posteriores.
- Compruebe que la máquina virtual esté apagada.

- Los hosts ESXi que se ejecuten en el entorno deben ser ESXi 6.7 o una versión posterior.
- La máquina virtual debe usar firmware EFI.
- Compruebe que dispone de los privilegios requeridos:
  - **Operaciones de cifrado.Clonar**
  - **Operaciones de cifrado.Cifrar**
  - **Operaciones de cifrado.Cifrar nuevo**
  - **Operaciones de cifrado.Registrar máquina virtual**

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual en el inventario que desee modificar y seleccione **Editar configuración**.

3 En el cuadro de diálogo **Editar configuración**, haga clic en **Agregar nuevo dispositivo** y seleccione **Módulo de plataforma de confianza**.

4 Haga clic en **Aceptar**.

La pestaña **Resumen** de la máquina virtual incluye ahora el Módulo de plataforma de confianza virtual en el panel **Hardware de máquina virtual**.

Quitar el módulo de plataforma de confianza virtual de una máquina virtual

Puede quitar la seguridad del módulo de plataforma de confianza (vTPM) de una máquina virtual.

Si se quita un dispositivo el vTPM, la información cifrada en la máquina virtual no se podrá recuperar. Antes de quitar un vTPM de una máquina virtual, deshabilite todas las aplicaciones en el sistema operativo invitado que utilicen el dispositivo vTPM, como BitLocker. Si no lo hace, es posible que la máquina virtual no arranque. Además, no es posible quitar un vTPM de una máquina virtual que contenga instantáneas.

Requisitos previos

- Compruebe que la máquina virtual esté apagada.
- Compruebe que dispone del privilegio necesario: **Operaciones de cifrado.Descifrar**

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual en el inventario que desee modificar y seleccione **Editar configuración**.

3 En el cuadro de diálogo **Editar configuración**, busque la entrada del Módulo de plataforma de confianza en la pestaña **Hardware virtual**.

4 Coloque el puntero sobre el dispositivo y haga clic en el icono **Quitar**.

Este icono solo aparece para el hardware virtual que se puede quitar de forma segura.

5 Haga clic en **Eliminar** para confirmar que desea quitar el dispositivo.

El dispositivo vTPM se marcará para su eliminación.

6 Haga clic en **Aceptar**.

Compruebe que la entrada del módulo de plataforma de confianza virtual ya no aparezca en la pestaña **Resumen** de la máquina virtual en el panel **Hardware de máquina virtual**.

Identificar las máquinas virtuales habilitadas para el módulo de la plataforma de confianza virtual

Puede identificar las máquinas virtuales habilitadas para el uso de un módulo de plataforma de confianza virtual (Virtual Trusted Platform Module, vTPM).

Puede generar una lista de todas las máquinas virtuales del inventario que incluya el nombre de la máquina virtual, el sistema operativo y el estado de vTPM. También puede exportar esta lista a un archivo CSV para su uso en auditorías de cumplimiento.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione una instancia de vCenter Server, un host o un clúster.

3 Haga clic en la pestaña **Máquinas virtuales** y seleccione **Máquinas virtuales**.

4 Haga clic en la barra de menú de cualquier columna de máquina virtual, seleccione **Mostrar/Ocultar columnas** y elija **TPM**.

La columna TPM se muestra como presente para todas las máquinas virtuales en las que se habilitó TPM. Las máquinas virtuales sin TPM se muestran como no presentes.

5 Puede exportar el contenido de una vista de lista de inventario a un archivo CSV.

a Haga clic en **Exportar** en la esquina inferior derecha de una vista de lista.

Se abre el cuadro de diálogo Exportar contenido de lista y muestra las opciones disponibles para incluir en el archivo CSV.

b Seleccione si quiere que todas las filas se incluyan en el archivo CSV o solamente las filas seleccionadas actualmente.

c En las opciones disponibles, seleccione la columnas que quiera que se incluyan en el archivo CSV.

d Haga clic en **Exportar**.

Se generará el archivo CSV para descargar.

Ver certificados de dispositivo del módulo de plataforma de confianza virtual

Los dispositivos del módulo de plataforma de confianza virtual (Virtual Trusted Platform Module, vTPM) están preconfigurados con certificados predeterminados, que pueden revisarse.

Requisitos previos

Debe haber una máquina virtual que admita vTPM en su entorno.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Haga clic en l**Máquinas virtuales** y seleccione **Máquinas virtuales**.

4 Seleccione la máquina virtual con el módulo vTPM habilitado cuya información de certificado desee ver.

   Si es necesario, haga clic en la barra de menú de cualquier columna de máquina virtual, seleccione **Mostrar/Ocultar columnas** y elija **TPM** para mostrar las máquinas virtuales con un TPM "Presente".

5 Haga clic en la pestaña **Configurar**.

6 En **TPM**, seleccione **Certificados**.

7 Seleccione el certificado y vea su información.

8 (Opcional) Para exportar la información del certificado, haga clic en **Exportar**.

   El certificado se guarda en el disco.

Pasos siguientes

Puede reemplazar el certificado predeterminado por un certificado emitido por una entidad de certificación de terceros (Certificate Authority, CA). Consulte Exportar y reemplazar certificados de dispositivo del Módulo de plataforma de confianza.

Exportar y reemplazar certificados de dispositivo del Módulo de plataforma de confianza

Puede reemplazar el certificado predeterminado incluido en el dispositivo del módulo de plataforma de confianza virtual (vTPM).

Requisitos previos

Debe haber una máquina virtual que admita vTPM en su entorno.

Procedimiento

1. Conéctese a vCenter Server mediante vSphere Client.
2. Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.
3. Seleccione la máquina virtual que admita vTPM en el inventario cuya información de certificado desee reemplazar.
4. Haga clic en la pestaña **Configurar**.
5. En **TPM**, seleccione **Solicitudes de firma**.
6. Seleccione un certificado.
7. Para exportar la información del certificado, haga clic en **Exportar**.

   El certificado se guarda en el disco.
8. Obtenga un certificado emitido por una entidad de certificación (Certificate Authority, CA) de terceros mediante la solicitud de firma del certificado (Certificate Signing Request, CSR) que exportó.

   Puede utilizar cualquier CA de prueba que tenga en el entorno de TI.
9. Cuando tenga el certificado nuevo, reemplace el certificado existente.

   a. Haga clic con el botón derecho en la máquina virtual en el inventario cuyo certificado desee modificar y seleccione **Editar configuración**.

   b. En el cuadro de **Editar configuración**, expanda **Dispositivos de seguridad** y, a continuación, expanda **Módulo de plataforma de confianza**.

      Aparecen los certificados.

   c. Haga clic en **Reemplazar** para el certificado que desea reemplazar.

      Aparece el cuadro de diálogo **Cargar archivo**.

   d. En la máquina local, busque el nuevo certificado y cárguelo.

      El nuevo certificado sustituye al certificado predeterminado que incluía el dispositivo vTPM.

   e. El nombre del certificado se actualizará en la pestaña **Resumen** de la máquina virtual en la lista **Módulo de plataforma de confianza virtual**.

Proteger sistemas operativos invitados Windows con seguridad basada en la virtualización 9

A partir de vSphere 6.7, puede habilitar la seguridad basada en la virtualización (Virtualization-Based Security, VBS) de Microsoft en los sistemas operativos invitados Windows admitidos.

Descripción de la seguridad basada en la virtualización

Microsoft VBS, una función de los sistemas operativos Windows 10 y Windows Server 2016, utiliza la virtualización de hardware y software para mejorar la seguridad del sistema mediante la creación de un subsistema aislado, especializado y restringido por el hipervisor.

VBS permite utilizar las siguientes funciones de seguridad de Windows a fin de proteger el sistema y aislar los datos confidenciales clave del sistema y del usuario para que no se vean comprometidos:

- Protección de credenciales: tiene como objetivo aislar y proteger datos confidenciales clave del sistema y del usuario frente a riesgos.
- Protección de dispositivos: proporciona un conjunto de funciones diseñadas para trabajar juntas con el fin de prevenir y eliminar el malware que se ejecuta en un sistema Windows.
- Integridad de código configurable: garantiza que solo se ejecute código de confianza desde el cargador de arranque en adelante.

Consulte el tema sobre la seguridad basada en la virtualización en la documentación de Microsoft para obtener más información.

Después de habilitar VBS para una máquina virtual a través de vCenter Server, debe habilitar VBS en el sistema operativo invitado Windows.

Este capítulo incluye los siguientes temas:

- Prácticas recomendadas de seguridad basada en virtualización
- Habilitar la seguridad basada en virtualización en una máquina virtual
- Habilitar la seguridad basada en virtualización en una máquina virtual existente
- Habilitar la seguridad basada en virtualización en el sistema operativo invitado
- Deshabilitar la seguridad basada en virtualización
- Identificar máquinas virtuales habilitadas para VBS

Prácticas recomendadas de seguridad basada en virtualización

Siga las prácticas recomendadas de VBS para maximizar la seguridad y la facilidad de administración del entorno de sistema operativo invitado Windows.

Evite problemas siguiendo estas prácticas recomendadas.

VBS de hardware

Utilice el siguiente hardware Intel de VBS:

- CPU Haswell o una versión posterior. Para obtener el mejor rendimiento, utilice la CPU Skylake-EP o una versión posterior.
- La CPU Ivy Bridge es aceptable.
- La CPU Sandy Bridge puede provocar un rendimiento lento.

No todas las funcionalidades de VBS están disponibles en las CPU de AMD. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/54009.

Compatibilidad de sistema operativo invitado Windows

VBS es compatible con máquinas virtuales con Windows 10, Windows Server 2016 y Windows Server 2019, aunque las versiones 1607 y 1703 de Windows Server 2016 requieren revisiones. Consulte la documentación de Microsoft sobre compatibilidad de hardware del host ESXi.

Para VBS en los sistemas operativos invitados Windows RS1, RS2 y RS3 se requiere que HyperV esté habilitado en el sistema operativo invitado. Para obtener más información, consulte *Notas de la versión de VMware vSphere*.

Funciones de VMware no admitidas en VBS

Las siguientes funciones no se admiten en una máquina virtual cuando se habilita VBS:

- Tolerancia a errores
- Acceso directo a PCI
- La adición en caliente de CPU o memoria

Las advertencias de instalación y actualización con VBS

Antes de configurar VBS, debe comprender las siguientes advertencias de instalación y actualización:

- Las máquinas virtuales nuevas configuradas para Windows 10, Windows Server 2016 y Windows Server 2019 en versiones de hardware inferiores a la versión 14 se deben crear mediante BIOS heredado de forma predeterminada. Debe volver a instalar el sistema operativo invitado después de cambiar el tipo de firmware de la máquina virtual desde el BIOS heredado a UEFI.
- Si va a migrar las máquinas virtuales de versiones anteriores de vSphere a vSphere 6.7 o una versión posterior y tiene pensado habilitar VBS en las máquinas virtuales, use UEFI para evitar tener que volver a instalar el sistema operativo.

Habilitar la seguridad basada en virtualización en una máquina virtual

Puede habilitar la VBS de Microsoft para sistemas operativos invitados Windows compatibles mientras crea una máquina virtual.

La habilitación de VBS es un proceso en el que primero se debe habilitar VBS en la máquina virtual y, posteriormente, en el sistema operativo invitado Windows.

Requisitos previos

Se recomienda utilizar hosts Intel. Consulte Prácticas recomendadas de seguridad basada en virtualización para conocer las CPU aceptables.

Cree una máquina virtual que utilice la versión de hardware 14 o posterior y uno de los siguientes sistemas operativos invitados compatibles:

- Windows 10 (64 bits)
- Windows Server 2016 (64 bits)
- Windows Server 2019 (64 bits)

Procedimiento

1. Conéctese a vCenter Server mediante vSphere Client.
2. Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Haga clic con el botón derecho en el objeto, seleccione **Nueva máquina virtual** y siga las indicaciones para crear una máquina virtual.

Opción	Acción
Seleccionar un tipo de creación	Cree una máquina virtual.
Seleccionar un nombre y una carpeta	Especifique un nombre y una ubicación de destino.
Seleccionar un recurso informático	Especifique el objeto sobre el que tiene privilegios para crear máquinas virtuales.
Seleccionar almacenamiento	En la directiva de almacenamiento de máquina virtual, seleccione la directiva de almacenamiento. Seleccione un almacén de datos compatible.
Seleccionar compatibilidad	Asegúrese de seleccionar **ESXi 6.7 y versiones posteriores**.
Seleccionar un sistema operativo invitado	Seleccione Windows 10 (64 bits), Windows Server 2016 (64 bits) o Windows Server 2019 (64 bits). Activar la casilla **Habilitar seguridad basada en virtualización de Windows**.
Personalizar hardware	Personalice el hardware, por ejemplo, cambiando el tamaño de disco o CPU.
Listo para finalizar	Revise la información y haga clic en **Finalizar**.

Resultados

Una vez creada la máquina virtual, confirme que la pestaña **Resumen** muestre “VBS true” en la descripción del sistema operativo invitado.

Pasos siguientes

Consulte Habilitar la seguridad basada en virtualización en el sistema operativo invitado.

Habilitar la seguridad basada en virtualización en una máquina virtual existente

Puede habilitar la VBS de Microsoft en las máquinas virtuales existentes para sistemas operativos invitados Windows admitidos.

La habilitación de VBS es un proceso en el que primero se debe habilitar VBS en la máquina virtual y, posteriormente, en el sistema operativo invitado.

Nota Las máquinas virtuales nuevas configuradas para Windows 10, Windows Server 2016 y Windows Server 2019 en versiones de hardware inferiores a la versión 14 se deben crear mediante BIOS heredado de forma predeterminada. Si cambia el tipo de firmware de la máquina virtual de BIOS heredado a UEFI, debe volver a instalar el sistema operativo invitado.

Requisitos previos

Se recomienda utilizar hosts Intel. Consulte Prácticas recomendadas de seguridad basada en virtualización para conocer las CPU aceptables.

La máquina virtual debe ser una creada con hardware versión 14 o posterior, firmware UEFI y uno de los siguientes sistemas operativos invitados compatibles:

- Windows 10 (64 bits)
- Windows Server 2016 (64 bits)
- Windows Server 2019 (64 bits)

Procedimiento

1. En vSphere Client, desplácese hasta la máquina virtual.
2. Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.
3. Haga clic en la pestaña **Opciones de máquina virtual**.
4. Active la casilla **Habilitar** para Seguridad basada en virtualización.
5. Haga clic en **Aceptar**.

Resultados

Confirme que la pestaña **Resumen** de la máquina virtual muestre "VBS true" en la descripción del sistema operativo invitado.

Pasos siguientes

Consulte Habilitar la seguridad basada en virtualización en el sistema operativo invitado.

Habilitar la seguridad basada en virtualización en el sistema operativo invitado

Puede habilitar la VBS de Microsoft para sistemas operativos invitados Windows admitidos.

Habilite VBS desde el sistema operativo invitado Windows. Windows configura y aplica VBS a través de un objeto de directiva de grupo (Group Policy Object, GPO). El objeto GPO ofrece la posibilidad de desactivar y activar los diversos servicios, como el arranque seguro, la protección de dispositivos y la protección de credenciales, que ofrece VBS. Ciertas versiones de Windows también requieren que se realice un paso adicional para habilitar la plataforma de Hyper-V.

Consulte la documentación de Microsoft sobre la implementación de la protección de dispositivos para habilitar la seguridad basada en virtualización si desea obtener más detalles.

Requisitos previos

- Asegúrese de que se haya habilitado la seguridad basada en virtualización en la máquina virtual.

Procedimiento

1. En Microsoft Windows, edite la directiva de grupo para activar VBS y elegir otras opciones de seguridad relacionadas con VBS.

2 (opcional) Para las versiones de Microsoft Windows inferiores a Redstone 4, en el panel de control Características de Windows, habilite la plataforma de Hyper-V.

3 Reinicie el sistema operativo invitado.

Deshabilitar la seguridad basada en virtualización

Si ya no utiliza VBS con una máquina virtual, puede deshabilitarla. Cuando se deshabilita VBS en la máquina virtual, las opciones de VBS de Windows permanecen sin modificaciones, pero pueden provocar problemas de rendimiento. Antes de deshabilitar VBS en la máquina virtual, deshabilite las opciones de VBS dentro de Windows.

Requisitos previos

Compruebe que la máquina virtual esté apagada.

Procedimiento

1 En vSphere Client, desplácese hasta la máquina virtual habilitada para VBS.

   Consulte Identificar máquinas virtuales habilitadas para VBS para obtener ayuda en la ubicación de máquinas virtuales habilitadas para VBS.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

3 Haga clic en **Opciones de máquina virtual**.

4 Anule la selección de la casilla **Habilitar** para Seguridad basada en virtualización.

   Un mensaje le recordará que debe deshabilitar VBS en el sistema operativo invitado.

5 Haga clic en **Aceptar**.

6 Compruebe que la pestaña **Resumen** de la máquina virtual ya no muestre “VBS true” en la descripción del sistema operativo invitado.

Identificar máquinas virtuales habilitadas para VBS

Puede identificar las máquinas virtuales que tienen la VBS habilitada para fines de cumplimiento y generación de informes.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un host, un centro de datos o una instancia de vCenter Server en el inventario.

3 Haga clic en la pestaña **Máquinas virtuales** y seleccione **Máquinas virtuales**.

4 En la lista de máquinas virtuales, haga clic en la flecha hacia abajo en un encabezado de columna para mostrar u ocultar columnas, y active la casilla **VBS**.

   Aparece la columna **VBS**.

5 Busque Presente en la columna **VBS**.

Proteger las redes de vSphere

10

La protección de las redes de vSphere es una parte fundamental de la seguridad del entorno. Los diferentes componentes de vSphere se protegen de varias maneras. Consulte la documentación de *Redes de vSphere* para obtener información detallada sobre las redes del entorno de vSphere.

Este capítulo incluye los siguientes temas:

- Introducción a la seguridad de red de vSphere
- Proteger la red con firewalls
- Proteger el conmutador físico
- Protección de puertos de conmutadores estándar con directivas de seguridad
- Proteger conmutadores estándar de vSphere
- Protección de conmutador estándar y VLAN
- Proteger conmutadores distribuidos y grupos de puertos distribuidos de vSphere
- Proteger las máquinas virtuales con VLAN
- Crear varias redes en un único host ESXi
- Seguridad del protocolo de Internet
- Garantizar la correcta configuración de SNMP
- Prácticas recomendadas de seguridad de redes de vSphere

Introducción a la seguridad de red de vSphere

La seguridad de red para el entorno de vSphere contiene muchas características similares a la protección de un entorno de red física, pero también incluye algunas otras que se aplican solamente a las máquinas virtuales.

Firewalls

Agregue protección de firewall a la red virtual mediante la instalación y la configuración de firewalls basados en host en algunas o todas las máquinas virtuales.

Para mejorar la eficiencia, puede configurar redes virtuales o redes Ethernet de máquinas virtuales privadas. En las redes virtuales, se instala un firewall basado en host en una máquina virtual en el encabezado de la red virtual. Este firewall funciona como búfer de protección entre el adaptador de red físico y las máquinas virtuales restantes de la red virtual.

Los firewalls basados en host pueden reducir el rendimiento. Equilibre las necesidades de seguridad con respecto a los objetivos de rendimiento antes de instalar firewalls basados en hosts en las máquinas virtuales en otro lugar de la red virtual.

Consulte Proteger la red con firewalls.

Segmentar

Mantenga las zonas de máquinas virtuales diferentes dentro de un host en distintos segmentos de red. Al aislar cada zona de máquinas virtuales en su propio segmento de red, es posible minimizar el riesgo de pérdidas de datos entre una zona y la siguiente. Con la segmentación se evitan diversas amenazas, incluida la suplantación del protocolo Address Resolution Protocol (ARP). Con la suplantación de ARP, un atacante manipula la tabla de ARP para reasignar las direcciones MAC e IP, y así obtener acceso al tráfico de red que va al host y procede de él. Los atacantes usan la suplantación de protocolo ARP para generar ataques de tipo "Man in the middle" (MITM), realizar ataques por denegación de servicio (DoS), secuestrar el sistema de destino y desestabilizar la red virtual de otras maneras.

Si la segmentación se planifica minuciosamente, se reducen las posibilidades de que se realicen transmisiones de paquetes entre las zonas de máquinas virtuales. Con la segmentación, por tanto, se evitan los ataques por analizadores de protocolos (sniffer), que se basan en el envío de tráfico de red a la víctima. Asimismo, un atacante no puede usar un servicio que no sea seguro en una zona de máquinas virtuales para acceder a otras zonas del host. El usuario puede elegir entre dos enfoques para implementar la segmentación.

- Use adaptadores de red físicos separados para las zonas de máquinas virtuales a fin de garantizar que las zonas queden aisladas. Probablemente, este método sea el más seguro después de la creación inicial del segmento. Este enfoque es también menos proclive a producir errores de configuración.
- Configure redes de área local virtuales (VLAN) para ayudar a proteger la red. Las VLAN proporcionan casi todas las ventajas de seguridad inherentes en la implementación de redes separadas físicamente sin generar una sobrecarga de hardware. Pueden ahorrarle el coste de tener que implementar y mantener otros dispositivos, el cableado, etc. Consulte Proteger las máquinas virtuales con VLAN.

Evitar el acceso no autorizado

Los requisitos de seguridad de las máquinas virtuales suelen ser los mismos que los de las máquinas físicas.

- Si una red de máquinas virtuales está conectada a una red física, puede quedar expuesta a infracciones, al igual que una red compuesta de máquinas físicas.

- Incluso si no conecta una máquina virtual a la red física, la máquina virtual puede recibir ataques de otras máquinas virtuales.

Las máquinas virtuales están aisladas entre sí. Una máquina virtual no puede leer ni escribir en la memoria de otra máquina virtual, acceder a sus datos, usar sus aplicaciones, etc. Sin embargo, dentro de la red, cualquier máquina virtual o un grupo de máquinas virtuales puede seguir siendo el destino del acceso no autorizado de otras máquinas virtuales. Proteja las máquinas virtuales de este tipo de acceso no autorizado.

Para obtener más información sobre cómo proteger las máquinas virtuales, consulte el documento de NIST llamado "Configuración de red virtual segura para la protección de máquinas virtuales (Virtual Machine, VM)" en:

https://csrc.nist.gov/publications/detail/sp/800-125b/final

Proteger la red con firewalls

Los administradores de seguridad usan firewalls para proteger la red o los componentes seleccionados en la red de las intromisiones.

Los firewalls controlan el acceso a los dispositivos dentro de su perímetro mediante el cierre de todos los puertos, excepto los puertos que el administrador designa explícita o implícitamente como autorizados. Los puertos que el administrador abre permiten el tráfico entre dispositivos en diferentes lados del firewall.

Importante El firewall de ESXi en ESXi 5.5 y versiones posteriores no permite filtrar el tráfico de vMotion por red. Por lo tanto, se deben instalar reglas en el firewall externo para que no se puedan establecer conexiones entrantes con el socket de vMotion.

En un entorno de máquina virtual, se puede planear la distribución de los firewalls entre los componentes.

- Firewalls entre máquinas físicas, tales como los sistemas vCenter Server y los hosts ESXi.
- Los firewalls entre una máquina virtual y otra, por ejemplo, entre una máquina virtual que actúa como servidor web externo y una máquina virtual conectada a la red interna de la empresa.
- Firewalls entre una máquina física y una máquina virtual, como cuando se coloca un firewall entre una tarjeta de adaptador de red física y una máquina virtual.

El modo de usar firewalls en la configuración de ESXi depende de cómo se planea utilizar la red y qué tan seguro debe ser un componente determinado. Por ejemplo, si crea una red virtual en la que cada máquina virtual está dedicada a ejecutar un conjunto de pruebas de referencia diferente para el mismo departamento, el riesgo de que se produzca un acceso no deseado de una máquina virtual a la siguiente es mínimo. Por lo tanto, no se necesita una configuración en la que haya firewalls entre las máquinas virtuales. Sin embargo, para evitar la interrupción de la ejecución de una prueba por parte de un host externo, puede configurar un firewall en el punto de entrada de la red virtual a fin de proteger todo el conjunto de máquinas virtuales.

Para ver un diagrama de los puertos de firewall, consulte el artículo 2131180 de la base de conocimientos de VMware.

Firewalls para configuraciones con vCenter Server

Si se accede a los hosts ESXi a través de vCenter Server, generalmente se protege vCenter Server con un firewall.

Los firewalls deben estar en el punto de entrada. El firewall puede estar entre los clientes y vCenter Server, o bien tanto vCenter Server como los clientes pueden estar detrás de un firewall.

Para obtener la lista de todos los puertos y protocolos compatibles en los productos de VMware, incluidos vSphere y vSAN, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/. Puede buscar puertos por producto de VMware, crear una lista de puertos personalizada e imprimir o guardar listas de puertos.

Las redes configuradas con vCenter Server pueden recibir comunicaciones a través de vSphere Web Client, otros clientes de UI o clientes que utilizan vSphere API. Durante el funcionamiento normal, vCenter Server escucha los datos de sus hosts y clientes administrados en los puertos designados. vCenter Server también asume que sus hosts administrados escuchan datos de vCenter Server en los puertos designados. Si hay un firewall entre cualquiera de estos elementos, el firewall debe tener puertos abiertos para admitir la transferencia de datos.

También se pueden incluir firewalls en otros puntos de acceso de la red, según el uso de la red y el nivel de seguridad que requieren los clientes. Seleccione las ubicaciones de los firewalls según los riesgos de seguridad de la configuración de red. Las siguientes ubicaciones de firewall se utilizan comúnmente.

- Entre vSphere Web Client o un cliente de administración de redes externo y vCenter Server.
- Si sus usuarios acceden a las máquinas virtuales a través de un explorador web, entre el explorador web y el host ESXi.
- Si sus usuarios acceden a las máquinas virtuales a través de vSphere Web Client, entre vSphere Web Client y el host ESXi. Esta conexión es adicional a la conexión entre vSphere Web Client y vCenter Server, y requiere un puerto diferente.
- Entre vCenter Server y los hosts ESXi.
- Entre los hosts ESXi de la red. A pesar de que el tráfico entre hosts generalmente se considera confiable, puede agregar firewalls entre ellos si sospecha que hay infracciones de seguridad entre una máquina y la otra.

  Si agrega firewalls entre hosts ESXi y tiene pensado migrar las máquinas virtuales entre ellos, abra los puertos en cualquier firewall que divida el host de origen de los host de destino.
- Entre los hosts ESXi y el almacenamiento de red, como el almacenamiento NFS o de iSCSI. Estos puertos no son exclusivos de VMware. Configúrelos de acuerdo con las especificaciones de la red.

Conexión con vCenter Server mediante un firewall

Abra el puerto TCP 443 en el firewall para que vCenter Server pueda recibir datos. De forma predeterminada, vCenter Server usa el puerto TCP 443 para escuchar la transferencia de datos de sus clientes. Si se usa un firewall entre vCenter Server y sus clientes, es necesario configurar una conexión a través de la cual vCenter Server pueda recibir los datos de sus clientes.

La configuración del firewall depende de lo que se use en el sitio. Solicite información al administrador del sistema de firewall local. La manera de abrir puertos depende de si se utiliza una instalación de Windows de vCenter Server Appliance o vCenter Server.

Conectar hosts ESXi mediante firewalls

Si tiene un firewall entre dos hosts ESXi y vCenter Server, asegúrese de que los hosts administrados puedan recibir datos.

Para configurar una conexión a fin de recibir datos, abra los puertos para el tráfico proveniente de los servicios, como vSphere High Availability, vMotion y vSphere Fault Tolerance. Consulte Configurar firewalls de ESXi para ver una explicación de los archivos de configuración, del acceso de vSphere Web Client y de los comandos de firewall. Consulte Puertos de firewall entrantes y salientes para hosts de ESXi para obtener una lista de los puertos.

Firewalls para configuraciones sin vCenter Server

Si el entorno no incluye vCenter Server, los clientes pueden conectarse directamente a la red ESXi.

Un host independiente ESXi se pueden conectar de varias formas.

- VMware Host Client
- Una de las interfaces de línea de comandos de vSphere
- vSphere Web Services SDK o vSphere Automation SDK
- Clientes de terceros

Los requisitos de firewall para los hosts independientes son similares a los requisitos aplicables cuando hay una instancia de vCenter Server.

- Utilice un firewall para proteger la capa ESXi o, según la configuración, los clientes y la capa ESXi. El firewall ofrece una protección básica para la red.
- La concesión de licencias en este tipo de configuración es parte del paquete de ESXi que instala en cada uno de los hosts. Debido a que la licencia reside en ESXi, no es necesario contar con un servidor de licencia distinto con un firewall.

Se pueden configurar puertos de firewall mediante ESXCLI o VMware Host Client. Consulte *Administrar un host único de vSphere: VMware Host Client*.

Conectar con la consola de la máquina virtual mediante un firewall

Algunos puertos deben estar abiertos para que el usuario y el administrador se comuniquen con la consola de la máquina virtual. Los puertos que deben estar abiertos dependen del tipo de consola de máquina virtual y de si se establece la conexión mediante vCenter Server con vSphere Web Client o directamente con el host ESXi desde VMware Host Client.

Conectarse a una consola de máquina virtual basada en explorador mediante vSphere Web Client

Cuando se conecta con vSphere Web Client, se conecta siempre al sistema vCenter Server que administra el host ESXi, y se accede desde allí a la consola de máquina virtual.

Si utiliza vSphere Web Client y se conecta a una consola de máquina virtual basada en explorador, el acceso siguiente debe ser posible:

- El firewall debe permitir que vSphere Web Client acceda a vCenter Server en el puerto 9443.
- El firewall debe permitir que vCenter Server acceda al host ESXi en el puerto 902.

Conectarse a VMware Remote Console mediante vSphere Web Client

Si utiliza vSphere Web Client y se conecta a VMware Remote Console (VMRC), el acceso siguiente debe ser posible:

- El firewall debe permitir que vSphere Web Client acceda a vCenter Server en el puerto 9443.
- El firewall debe permitir que la máquina virtual independiente acceda a vCenter Server en el puerto 9443 y al host ESXi en el puerto 902 en las versiones de VMRC anteriores a 11.0, y en el puerto 443 en la versión 11.0 y posteriores de VMRC. Para obtener más información sobre la versión 11.0 de VMRC y los requisitos de puerto de ESXi, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/76672.

Conexión directa a hosts ESXi con VMware Host Client

Es posible utilizar la consola de máquina virtual de VMware Host Client si se conecta directamente a un host ESXi.

Nota No utilice VMware Host Client para conectarse directamente a hosts administrados por un sistema vCenter Server. Si hace cambios en esos hosts desde VMware Host Client, se producirá inestabilidad en el entorno.

El firewall debe permitir el acceso al host ESXi en los puertos 443 y 902

VMware Host Client utiliza el puerto 902 para ofrecer una conexión para las actividades de MKS del sistema operativo invitado en las máquinas virtuales. A través de este puerto, los usuarios interactúan con los sistemas operativos invitados y las aplicaciones de la máquina virtual. VMware no admite la configuración de otro puerto para esta función.

Proteger el conmutador físico

Proteja el conmutador físico de cada host ESXi para evitar que los atacantes tengan acceso al host y sus máquinas virtuales.

Para optimizar la protección de los hosts, compruebe que los puertos de conmutadores físicos estén configurados con el árbol de expansión deshabilitado, y que la opción de no negociación esté configurada para los vínculos troncales entre conmutadores físicos externos y conmutadores virtuales en el modo de etiquetado de conmutador virtual (VST).

Procedimiento

1 Inicie sesión en el conmutador físico y compruebe que el protocolo de árbol de expansión esté deshabilitado o que Port Fast esté configurado para todos los puertos de conmutadores físicos conectados a los hosts ESXi.

2 Para las máquinas virtuales que hacen puente y enrutamiento, compruebe periódicamente que el primer puerto de conmutador físico ascendente esté configurado con las opciones BPDU Guard y Port Fast deshabilitadas, y con el protocolo de árbol de expansión habilitado.

   En vSphere 5.1 y versiones posteriores, para evitar ataques potenciales de denegación de servicio (DoS) en el conmutador físico, puede activar el filtro de BPDU invitado en los hosts ESXi.

3 Inicie sesión en el conmutador físico y asegúrese de que el protocolo Dynamic Trunking Protocol (DTP) no esté habilitado en los puertos de conmutadores físicos conectados a los hosts ESXi.

4 De forma regular, revise los puertos de conmutadores físicos para asegurarse de que estén correctamente configurados como puertos troncales si están conectados a los puertos de enlace troncal de VLAN de conmutadores virtuales.

Protección de puertos de conmutadores estándar con directivas de seguridad

El grupo de puertos de VMkernel o el grupo de puertos de máquinas virtuales de un conmutador estándar tienen una directiva de seguridad configurable. La directiva de seguridad determina el nivel de seguridad con que se aplica la protección contra ataques de suplantación o intercepción en máquinas virtuales.

Al igual que ocurre con los adaptadores de red física, los adaptadores de red de máquina virtual pueden suplantar otra máquina virtual. La suplantación es un riesgo de seguridad.

- Una máquina virtual puede enviar tramas que parezcan ser de otra máquina de modo que reciba tramas de la red que estén destinadas a esa máquina.
- Un adaptador de red de máquina virtual puede configurarse para que reciba tramas destinadas a otras máquinas.

Al agregar un grupo de puertos VMkernel o un grupo de puertos de máquinas virtuales a un conmutador estándar, ESXi configura una directiva de seguridad para los puertos del grupo. Esta directiva de seguridad se puede utilizar para garantizar que el host evite que los sistemas operativos invitados de sus máquinas virtuales suplanten a otras máquinas en la red. El sistema operativo invitado que lleve a cabo la suplantación no detectará que se evitó la suplantación.

La directiva de seguridad determina el nivel de seguridad con que se aplica la protección contra ataques de suplantación o intercepción en máquinas virtuales. Para utilizar correctamente la configuración en el perfil de seguridad, consulte la sección de la directiva de seguridad en la publicación *Redes de vSphere*. En esta sección se explica:

- El modo en el que los adaptadores de red de máquina virtual controlan las transmisiones.
- El modo en el que se manipulan los ataques en este nivel.

Proteger conmutadores estándar de vSphere

Puede proteger el tráfico del conmutador estándar contra ataques de Capa 2 restringiendo algunos de los modos de dirección MAC de los adaptadores de red de máquina virtual.

Cada adaptador de red de máquina virtual tiene una dirección MAC inicial y una dirección MAC efectiva.

Dirección MAC inicial

La dirección MAC inicial se asigna con la creación del adaptador. Si bien la dirección MAC inicial puede volver a configurarse desde afuera del sistema operativo invitado, este sistema no puede modificarla.

Dirección MAC efectiva

Cada adaptador tiene una dirección MAC efectiva que filtra el tráfico de red entrante con una dirección MAC de destino distinta de la dirección MAC efectiva. El sistema operativo invitado es responsable de configurar la dirección MAC efectiva y, por lo general, hace coincidir la dirección MAC efectiva con la dirección MAC inicial.

Al crear un adaptador de red de máquina virtual, la dirección MAC efectiva y la dirección MAC inicial son iguales. El sistema operativo invitado puede modificar la dirección MAC efectiva con otro valor en cualquier momento. Si el sistema operativo modifica la dirección MAC efectiva, su adaptador de red recibe el tráfico de red destinado para la nueva dirección MAC.

Cuando se envían paquetes a través del adaptador de red, el sistema operativo invitado por lo general coloca su propia dirección MAC efectiva de adaptador en el campo de la dirección MAC de origen de las tramas Ethernet. Coloca la dirección MAC del adaptador de red receptor en el campo de la dirección MAC de destino. El adaptador receptor acepta los paquetes únicamente si la dirección MAC de destino del paquete coincide con su propia dirección MAC efectiva.

El sistema operativo puede enviar tramas con una dirección MAC de origen suplantada. Por lo tanto, un sistema operativo puede suplantar a un adaptador de red que haya autorizado la red receptora y llevar a cabo ataques maliciosos en los dispositivos de una red.

Puede proteger el tráfico virtual contra ataques de suplantación e intercepción de la Capa 2 si configura una directiva de seguridad en los puertos o grupos de puertos.

La directiva de seguridad en los puertos y grupos de puertos distribuidos incluye las siguientes opciones:

- Cambios en la dirección MAC (consulte Cambios de dirección MAC).
- Modo promiscuo (consulte Operación en modo promiscuo).
- Transmisiones falsificadas (consulte Transmisiones falsificadas).

Puede ver y cambiar la configuración predeterminada si selecciona el conmutador virtual asociado con el host desde vSphere Client. Consulte el documento *Redes de vSphere*.

Cambios de dirección MAC

La directiva de seguridad de un conmutador virtual incluye la opción **Cambios de dirección MAC**. Esta opción afecta el tráfico que recibe una máquina virtual.

Cuando la opción **Cambios de dirección MAC** está establecida en **Aceptar**, ESXi acepta las solicitudes de cambiar la dirección MAC efectiva por una dirección diferente a la inicial.

Cuando la opción **Cambios de dirección MAC** está establecida en **Rechazar**, ESXi no admite las solicitudes de cambiar la dirección MAC efectiva por una dirección diferente a la inicial. Esta configuración protege el host de la suplantación de MAC. El puerto que utilizó el adaptador de la máquina virtual para enviar la solicitud se deshabilita, y el adaptador de la máquina virtual no recibe más tramas hasta que la dirección MAC efectiva coincida con la dirección MAC inicial. El sistema operativo invitado no detecta el rechazo de la solicitud de cambio de dirección MAC.

Nota El iniciador iSCSI confía en poder obtener los cambios en la dirección MAC a partir de determinados tipos de almacenamiento. Si utiliza iSCSI de ESXi con almacenamiento iSCSI, establezca la opción **Cambios de dirección MAC** en **Aceptar**.

En ciertos casos, es posible que realmente necesite que más de un adaptador tenga la misma dirección MAC en una red (por ejemplo, si utiliza el equilibrio de carga de red de Microsoft en modo de unidifusión). Cuando el equilibrio de carga de red de Microsoft se utiliza en el modo de multidifusión estándar, los adaptadores no comparten las direcciones MAC.

Transmisiones falsificadas

La opción **Transmisiones falsificadas** afecta el tráfico que se transmite desde una máquina virtual.

Cuando la opción **Transmisiones falsificadas** está establecida en **Aceptar**, ESXi no compara las direcciones MAC de origen y efectivas.

Para evitar la suplantación de MAC, puede establecer la opción **Transmisiones falsificadas** en **Rechazar**. Si lo hace, el host compara la dirección MAC de origen que transmite el sistema operativo invitado con la dirección MAC efectiva de su adaptador de máquina virtual para ver si coinciden. Si las direcciones no coinciden, el host ESXi descarta el paquete.

El sistema operativo invitado no detecta que su adaptador de máquina virtual no puede enviar paquetes con la dirección MAC suplantada. El host ESXi intercepta los paquetes con direcciones suplantadas antes de que estos se envíen, y el sistema operativo invitado puede asumir que los paquetes se descartan.

Operación en modo promiscuo

El modo promiscuo quita el filtrado de recepción que realiza el adaptador de la máquina virtual a fin de que el sistema operativo invitado reciba todo el tráfico que se observa en la conexión. De forma predeterminada, el adaptador de la máquina virtual no puede operar en modo promiscuo.

A pesar de que el modo promiscuo puede ser útil para hacer un seguimiento de la actividad de la red, es un modo de operación no seguro, ya que cualquier adaptador en modo promiscuo tiene acceso a los paquetes, incluso si algunos de estos paquetes se reciben solamente en un adaptador de red en particular. Esto significa que un administrador o un usuario raíz que estén en una máquina virtual pueden ver potencialmente el tráfico destinado a otros sistemas operativos host o invitados.

Consulte el tema sobre cómo configurar la directiva de seguridad para un conmutador estándar de vSphere o un grupo de puertos estándar en la documentación de *Redes de vSphere*, para obtener información sobre cómo configurar el adaptador de máquina virtual para el modo promiscuo.

Nota En ciertas ocasiones, es posible que tenga una razón válida para configurar un conmutador virtual estándar o distribuido para operar en modo promiscuo, por ejemplo, si está ejecutando un software de detección de intrusiones de red o un analizador de protocolos (sniffer).

Protección de conmutador estándar y VLAN

Los conmutadores estándar de VMware ofrecen elementos de protección contra ciertas amenazas para la seguridad de VLAN. Debido a la forma en que se diseñan, los conmutadores estándar protegen las VLAN contra una variedad de ataques, muchos de los cuales implican saltos de VLAN.

Contar con esta protección no garantiza que la configuración de la máquina virtual sea invulnerable a otros tipos de ataques. Por ejemplo, los conmutadores estándar no protegen la red física frente a estos ataques: protegen solo la red virtual.

Los conmutadores estándar y las VLAN pueden ofrecer protección contra los siguientes tipos de ataques.

desbordamiento de MAC

Se desborda un conmutador con paquetes que contienen direcciones MAC etiquetadas como provenientes de diferentes orígenes. Muchos conmutadores utilizan una tabla de memoria de contenido direccionable que permite conocer y almacenar la dirección de origen para cada paquete. Cuando la tabla está completa, el conmutador puede entrar en un estado completamente abierto en el que todos los paquetes entrantes se difunden a todos los

puertos; esto permite al atacante ver todo el tráfico del conmutador. Dicho estado puede resultar en la pérdida de paquetes en todas las VLAN.

Aunque los conmutadores estándar de VMware almacenan una tabla de direcciones MAC, no obtienen estas del tráfico observable y no son vulnerables a este tipo de ataque.

ataques de etiquetado de ISL y 802.1Q

Se fuerza un conmutador a redirigir las tramas de una VLAN a otra; para ello, se engaña al conmutador para que actúe como un enlace troncal y difunda el tráfico hacia otras VLAN.

Los conmutadores estándar de VMware no llevan a cabo el enlace troncal dinámico requerido para este tipo de ataque y, por lo tanto, no son vulnerables.

Ataques de doble encapsulación

Se producen cuando un atacante crea un paquete de doble encapsulado donde el identificador de VLAN en la etiqueta interior es diferente del identificador de VLAN en la etiqueta exterior. Para lograr la compatibilidad con versiones anteriores, las VLAN nativas quitan la etiqueta exterior de los paquetes transmitidos a menos que se configure de otro modo. Cuando un conmutador de VLAN nativa quita la etiqueta exterior, queda solo la etiqueta interior, que enruta el paquete a una VLAN diferente de la que está identificada en la etiqueta exterior ahora faltante.

Los conmutadores estándar de VMware sueltan todas las tramas de doble encapsulado que una máquina virtual intenta enviar y lo hacen en un puerto configurado para una VLAN específica. Por lo tanto, no son vulnerables a este tipo de ataque.

Ataques de fuerza bruta de multidifusión

Implican el envío de gran cantidad de tramas de multidifusión a una VLAN conocida casi al mismo tiempo a fin de sobrecargar el conmutador de modo que, por error, permita que algunas de las tramas se difundan a otras VLAN.

Los conmutadores estándar de VMware no permiten que las tramas abandonen el dominio de difusión correcto (VLAN) y no son vulnerables a este tipo de ataque.

Ataques de árbol de expansión

Se trata del protocolo Spanning-Tree Protocol (STP) de destino, que se utiliza para controlar el puente entre las partes de la red LAN. El atacante envía paquetes de Bridge Protocol Data Unit (BPDU) que intentan cambiar la topología de la red y se establecen a sí mismos como el puente raíz. Como puente raíz, el atacante puede capturar el contenido de las tramas difundidas.

Los conmutadores estándar de VMware no son compatibles con el protocolo STP y no son vulnerables a este tipo de ataque.

Ataques de trama aleatoria

Implican enviar grandes cantidades de paquetes donde las direcciones de origen y destino permanecen iguales, pero se cambia de forma aleatoria la longitud, el tipo o el contenido de

los campos. El objetivo de este ataque es forzar a los paquetes a que, por error, se vuelvan a enrutar a una VLAN diferente.

Los conmutadores estándar de VMware no son vulnerables a este tipo de ataque.

Debido a que con el tiempo surgen nuevas amenazas de seguridad, no considere que esta lista de ataques está completa. Revise con regularidad los recursos de seguridad de VMware en la Web para obtener información sobre seguridad, alertas de seguridad recientes y tácticas de seguridad de VMware.

Proteger conmutadores distribuidos y grupos de puertos distribuidos de vSphere

Los administradores tienen varias opciones para proteger instancias de vSphere Distributed Switch en el entorno de vSphere.

Las mismas reglas se aplican a las VLAN tanto en una instancia de vSphere Distributed Switch como en un conmutador estándar. Para obtener más información, consulte Protección de conmutador estándar y VLAN.

Procedimiento

1 Para los grupos de puertos distribuidos con enlace estático, deshabilite la característica de expansión automática.

   Expansión automática está habilitada de forma predeterminada en vSphere 5.1 y versiones posteriores.

   Para habilitar Expansión automática, configure la propiedad `autoExpand` en el grupo de puertos distribuidos con vSphere Web Services SDK o con una interfaz de línea de comandos. Consulte la documentación de *vSphere Web Services SDK*.

2 Asegúrese de que todos los identificadores de VLAN privadas de vSphere Distributed Switch estén documentados detalladamente.

3 Si utiliza el etiquetado de VLAN en un dvPortgroup, los identificador de VLAN deben coincidir con los identificadores de los conmutadores ascendentes externos con reconocimiento de VLAN. Si los identificadores de VLAN no están registrados correctamente, la reutilización incorrecta de identificadores puede permitir tráfico no deseado. De forma similar, la presencia de identificadores de VLAN incorrectos o faltantes puede hacer que el tráfico no pase entre las máquinas físicas y virtuales.

4 Asegúrese de que no haya puertos sin utilizar en un grupo de puertos virtuales asociado con vSphere Distributed Switch.

5 Etiquete todos los conmutadores distribuidos de vSphere.

   Los conmutadores distribuidos de vSphere asociados con un host ESXi requieren un cuadro de texto para sus nombres. Esta etiqueta sirve como descriptor funcional del conmutador, al igual que el nombre de host asociado con un conmutador físico. La etiqueta de vSphere

Distributed Switch indica la función o la subred IP del conmutador Por ejemplo, puede etiquetar el conmutador como interno para indicar que solo sirve para las redes internas del conmutador virtual privado de una máquina virtual. El tráfico no pasa a través de los adaptadores de red física.

6 Deshabilite la comprobación de estado de la red en los conmutadores distribuidos de vSphere si no la utiliza de forma activa.

   La comprobación de estado de la red está deshabilitada de forma predeterminada. Una vez habilitados, los paquetes de comprobación de estado contienen información sobre el host, el conmutador y el puerto que un atacante podría utilizar. Utilice la comprobación de estado de la red solo para tareas de solución de problemas y desactívela al finalizar.

7 Puede proteger el tráfico virtual contra ataques de suplantación e intercepción de la Capa 2 si configura una directiva de seguridad en los puertos o grupos de puertos.

   La directiva de seguridad en los puertos y grupos de puertos distribuidos incluye las siguientes opciones:

   - Cambios en la dirección MAC (consulte Cambios de dirección MAC).
   - Modo promiscuo (consulte Operación en modo promiscuo).
   - Transmisiones falsificadas (consulte Transmisiones falsificadas).

   Para ver y cambiar la configuración actual, seleccione **Administrar grupos de puertos distribuidos** en el menú contextual y, a continuación, seleccione **Seguridad** en el asistente. Consulte la documentación de *Redes de vSphere*.

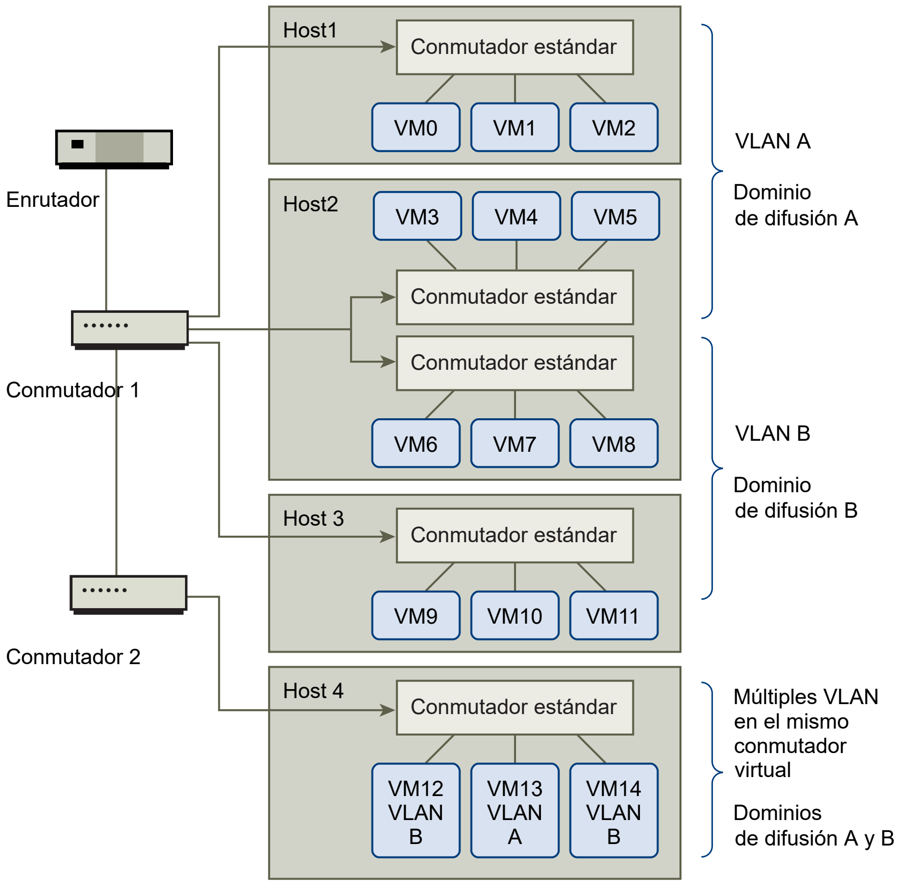
Proteger las máquinas virtuales con VLAN

La red puede ser una de las partes más vulnerables de un sistema. La red de máquinas virtuales necesita tanta protección como una red física. La utilización de VLAN puede mejorar la seguridad de las redes del entorno.

Las VLAN se encuentran en un esquema de redes estándar IEEE, con métodos de etiquetado específicos que permiten el enrutamiento de los paquetes únicamente hacia los puertos que forman parte de la VLAN. Cuando se las configura correctamente, las VLAN constituyen un medio confiable para proteger un conjunto de máquinas virtuales contra intrusiones accidentales o maliciosas.

Las VLAN permiten segmentar una red física de modo que dos máquinas de la red no puedan transmitirse paquetes entre ellas a menos que formen parte de la misma VLAN. Por ejemplo, las transacciones y los registros contables son algunos de los datos internos más confidenciales de una empresa. En una empresa cuyos empleados de los departamentos de ventas, envíos y contabilidad utilizan máquinas virtuales en la misma red física, es posible proteger las máquinas virtuales del departamento contable mediante la configuración de las VLAN.

Figura 10-1. Esquema de muestra de una VLAN



En esta configuración, todos los empleados del departamento contable utilizan máquinas virtuales en la VLAN A y los empleados de ventas utilizan máquinas virtuales en la VLAN B.

El enrutador reenvía los paquetes que contienen los datos contables a los conmutadores. Estos paquetes se etiquetan para la distribución en la VLAN A únicamente. Por lo tanto, los datos quedan confinados al dominio de difusión A y no pueden enrutarse al dominio de difusión B a menos que se configure al enrutador para hacerlo.

Esta configuración de VLAN impide que los empleados de ventas intercepten los paquetes destinados al departamento contable. También evita que el departamento contable reciba paquetes destinados al grupo de ventas. Las máquinas virtuales atendidas por un único conmutador virtual pueden encontrarse en diferentes VLAN.

Consideraciones de seguridad para VLAN

La forma de configurar VLAN para proteger partes de una red depende de factores tales como el sistema operativo invitado y el tipo de configuración del equipo de red.

ESXi cuenta con una implementación completa de VLAN compatibles con IEEE 802.1q VLAN. VMware no puede hacer recomendaciones específicas sobre el modo de configurar las VLAN, pero hay algunos factores que deben considerarse al usar la implementación de VLAN como parte de la directiva de cumplimiento de seguridad.

Proteger las VLAN

Los administradores tienen varias opciones para proteger las VLAN en el entorno de vSphere.

Procedimiento

1 Asegúrese de que los grupos de puertos no estén configurados con valores de la VLAN reservados para los conmutadores físicos ascendentes.

   No establezca los identificadores de la VLAN con valores reservados para el conmutador físico.

2 Compruebe que los grupos de puertos no estén configurados en la VLAN 4095 a menos que esté utilizando el etiquetado de invitado virtual (VGT).

   Hay tres tipos de etiquetado de VLAN en vSphere:

   - Etiquetado de conmutador externo (EST)
   - Etiquetado de conmutador virtual (VST): el conmutador virtual etiqueta con el identificador de VLAN configurado el tráfico que entra en las máquinas virtuales asociadas y quita la etiqueta de VLAN del tráfico saliente. Para configurar el modo VST, asigne un identificador de VLAN entre 1 y 4095.
   - Etiquetado de invitado virtual (VGT): las máquinas virtuales controlan el tráfico de VLAN. Para activar el modo VGT, establezca el identificador de VLAN en 4095. En un conmutador distribuido, también puede permitir el tráfico de máquinas virtuales en función de su VLAN mediante la opción **Enlace troncal de VLAN**.

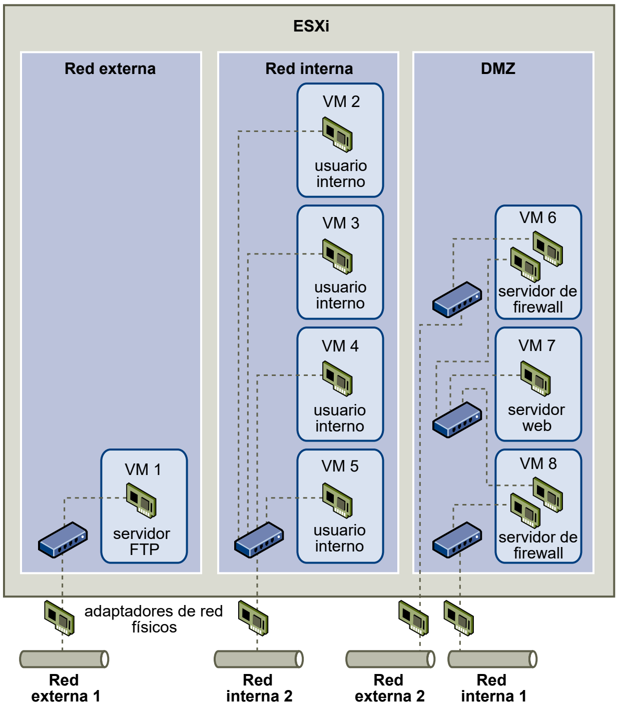
   En un conmutador estándar, puede configurar el modo de redes de VLAN en el nivel del conmutador o del grupo de puertos. En un conmutador distribuido, puede hacerlo en el nivel del puerto o del grupo de puertos distribuidos.

3 Asegúrese de que todas las VLAN de cada conmutador virtual estén completamente documentadas y que cada conmutador virtual tenga todas las VLAN requeridas y solamente esas.

Crear varias redes en un único host ESXi

El diseño del sistema ESXi permite conectar algunos grupos de máquinas virtuales a la red interna, otros a la red externa y otros a ambos, todos en el mismo host. Esta capacidad es una extensión del aislamiento básico de máquinas virtuales combinado con la utilización bien planificada de características de redes virtuales.

Figura 10-2. Redes externas, redes internas y una DMZ configuradas en un único host ESXi



En la figura, el administrador de sistema configuró un host en tres zonas de máquinas virtuales diferentes: servidor FTP, máquinas virtuales internas y DMZ. Cada zona tiene una función única.

Servidor FTP

La máquina virtual 1 está configurada con el software FTP y actúa como área de retención de los datos enviados hacia los recursos externos y desde estos, como formularios y documentación localizados por un proveedor.

Esta máquina virtual solo está asociada con una red externa. Tiene su propio conmutador virtual y su propio adaptador de red físico que la conectan a la red externa 1. Esta red está dedicada a los servidores que usa la empresa para recibir datos de orígenes externos. Por ejemplo, la empresa utiliza la red externa 1 para recibir tráfico FTP de los proveedores, y permite a estos últimos acceder a los datos almacenados en servidores disponibles de forma externa a través de FTP. Además de atender a la máquina virtual 1, la red externa 1 se encarga de los servidores FTP configurados en diferentes hosts ESXi en todo el sitio.

Debido a que la máquina virtual 1 no comparte un conmutador virtual o un adaptador de red físico con ninguna máquina virtual del host, las otras máquinas virtuales residentes no pueden transmitir paquetes a la red de la máquina virtual 1 ni recibir paquetes de ella. Esta restricción evita los ataques por analizadores de protocolos (sniffer), que se basan en el envío de tráfico de red a la víctima. Otro factor más importante es que un atacante no puede utilizar la vulnerabilidad natural de FTP para acceder a ninguna de las otras máquinas virtuales del host.

Máquinas virtuales internas

Las máquinas virtuales 2 a 5 están reservadas para la utilización interna. Estas máquinas virtuales procesan y almacenan datos privados de la empresa, como registros médicos, declaraciones legales e investigaciones de fraude. Por lo tanto, los administradores del sistema deben garantizar el nivel más alto de protección de estas máquinas virtuales.

Estas máquinas virtuales se conectan a la red interna 2 mediante un conmutador virtual y un adaptador de red propios. La red interna 2 está reservada para la utilización interna por parte del personal, por ejemplo, procesadores de reclamos, abogados internos o tasadores.

Las máquinas virtuales 2 a 5 pueden comunicarse entre sí mediante el conmutador virtual, y con máquinas internas de otros lugares de la red interna 2 mediante el adaptador de red físico. Sin embargo, no pueden comunicarse con máquinas externas. Al igual que con el servidor FTP, estas máquinas virtuales no pueden enviar paquetes a las redes de las otras máquinas virtuales ni recibir paquetes de ellas. De forma similar, las otras máquinas virtuales del host no pueden enviar paquetes a las máquinas virtuales 2 a 5 ni recibir paquetes de ellas.

DMZ

Las máquinas virtuales 6 a 8 se configuran como una DMZ que utiliza el grupo de comercialización para publicar el sitio web externo de la empresa.

Este grupo de máquinas virtuales se asocia con la red externa 2 y la red interna 1. La empresa utiliza la red externa 2 para admitir los servidores web que utilizan los departamentos de comercialización y finanzas para alojar el sitio web de la empresa y otras características web para usuarios externos. La red interna 1 es el medio que utiliza el departamento de comercialización para publicar contenido en el sitio web de la empresa, publicar descargas y mantener servicios como los foros de usuarios.

Debido a que estas redes están separadas de la red externa 1 y la red interna 2, y las máquinas virtuales no tienen puntos de contacto compartidos (conmutadores o adaptadores), no existe riesgo de ataque hacia o desde el servidor FTP o el grupo de máquinas virtuales internas.

Al lograr el aislamiento de máquinas virtuales, configurar correctamente los conmutadores virtuales y mantener la separación de las redes, el administrador del sistema puede alojar las tres zonas de máquinas virtuales en el mismo host ESXi y estar seguro de que no se producirán infracciones de datos o recursos.

La empresa aplica el aislamiento en los grupos de máquinas virtuales mediante la utilización de varias redes internas y externas, y se asegura de que los conmutadores virtuales y los adaptadores de red físicos de cada grupo se encuentren separados de esos grupos o de otros.

Gracias a que ninguno de estos conmutadores virtuales favorece zonas de máquinas virtuales sobre las demás, el administrador del sistema logra eliminar el riesgo de pérdida de paquetes de una zona a la otra. Debido a su diseño, un conmutador virtual no puede perder paquetes directamente en otro conmutador virtual. La única forma de que los paquetes pasen de un conmutador virtual a otro es en estas circunstancias:

- Los conmutadores virtuales están conectados a la misma LAN física.
- Los conmutadores virtuales se conectan a una máquina virtual común, que se puede utilizar para transmitir paquetes.

Ninguna de estas condiciones se cumple en la configuración de ejemplo. Si los administradores del sistema quieren comprobar que no existen rutas de acceso a conmutadores virtuales comunes, pueden revisar la distribución de conmutadores de red de vSphere Client para buscar posibles puntos de contacto compartidos.

Para proteger los recursos de las máquinas virtuales, el administrador del sistema disminuye el riesgo de ataques DoS y DDoS mediante la configuración de una reserva de recursos y un límite para cada máquina virtual. El administrador del sistema protege aún más el host y las máquinas virtuales de ESXi mediante la instalación de firewalls de software en los extremos delanteros y traseros de la DMZ, que garantiza que el host esté detrás de un firewall físico, y la configuración de los recursos de almacenamiento en red para que cada uno de ellos tenga su propio conmutador virtual.

Seguridad del protocolo de Internet

El protocolo Internet Protocol Security (IPsec) protege las comunicaciones de IP que recibe y envía un host. Los hosts ESXi admiten IPsec con IPv6.

Al configurar IPsec en un host, se habilita la autenticación y el cifrado de paquetes entrantes y salientes. El momento y el modo en que el tráfico de IP se cifra dependen de la configuración de las asociaciones de seguridad del sistema y de las directivas de seguridad.

Una asociación de seguridad determina el modo en que el sistema cifra el tráfico. Al crear una asociación de seguridad, se especifican el origen y el destino, los parámetros de cifrado y un nombre para la asociación de seguridad.

Una directiva de seguridad determina el momento en el que el sistema debe cifrar el tráfico. La directiva de seguridad incluye la información del origen y destino, el protocolo y la dirección del tráfico que se va a cifrar, el modo (transporte o túnel) y la asociación de seguridad que se deben utilizar.

Lista de asociaciones de seguridad disponibles

ESXi puede proporcionar una lista de todas las asociaciones de seguridad disponibles que pueden usar las directivas de seguridad. La lista incluye tanto las asociaciones de seguridad creadas por el usuario como las asociaciones de seguridad que haya instalado el VMkernel con el intercambio de claves por red.

Puede obtener una lista de las asociaciones de seguridad disponibles mediante el comando de vSphere CLI `esxcli`.

Procedimiento

- En el símbolo del sistema, introduzca el comando **`esxcli network ip ipsec sa list`**.

Resultados

ESXi muestra una lista de todas las asociaciones de seguridad disponibles.

Agregar una asociación de seguridad IPsec

Agregue una asociación de seguridad a fin de especificar parámetros de cifrado para el tráfico de IP asociado.

Puede agregar una asociación de seguridad mediante el comando `esxcli` de vSphere CLI.

Procedimiento

- En el símbolo del sistema, introduzca el comando **`esxcli network ip ipsec sa add`** con una o más de las siguientes opciones.

Opción	Descripción
`--sa-source=` *source address*	Requerido. Especifique la dirección de origen.
`--sa-destination=` *destination address*	Requerido. Especifique la dirección de destino.
`--sa-mode=` *mode*	Requerido. Especifique el modo, ya sea `transport` o `tunnel`.
`--sa-spi=` *security parameter index*	Requerido. Especifique el índice de parámetros de seguridad. El índice de parámetros de seguridad identifica la asociación de seguridad con el host. Debe ser un número hexadecimal con un prefijo 0x. Cada asociación de seguridad que cree debe tener una combinación única de protocolo e índice de parámetros de seguridad.
`--encryption-algorithm=` *encryption algorithm*	Requerido. Especifique el algoritmo de cifrado mediante uno de los siguientes parámetros. ■ `3des-cbc` ■ `aes128-cbc` ■ `null` (no proporciona cifrado)
`--encryption-key=` *encryption key*	Requerido al especificar un algoritmo de cifrado. Especifique la clave de cifrado. Puede introducir claves como texto ASCII o un número hexadecimal con un prefijo 0x.
`--integrity-algorithm=` *authentication algorithm*	Requerido. Especifique el algoritmo de autenticación, ya sea `hmac-sha1` o `hmac-sha2-256`.
`--integrity-key=` *authentication key*	Requerido. Especifique la clave de autenticación. Puede introducir claves como texto ASCII o un número hexadecimal con un prefijo 0x.
`--sa-name=`*name*	Requerido. Proporcione un nombre para la asociación de seguridad.

Ejemplo: Nuevo comando de asociación de seguridad

El siguiente ejemplo contiene saltos de línea adicionales para facilitar la lectura.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x6970763672656164796c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
```

```
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sa1
```

Quitar una asociación de seguridad IPsec

Es posible eliminar una asociación de seguridad mediante el comando ESXCLI de vSphere CLI.

Requisitos previos

Compruebe que la asociación de seguridad que desea utilizar no esté en uso. Si intenta eliminar una asociación de seguridad en uso, la operación de eliminación generará errores.

Procedimiento

- En el símbolo del sistema, introduzca el comando **esxcli network ip ipsec sa remove --sa-name** ***security_association_name***

Lista de directivas de seguridad IPsec disponibles

Las directivas de seguridad disponibles se pueden enumerar mediante el comando ESXCLI de vSphere CLI.

Procedimiento

- En el símbolo del sistema, introduzca el comando **esxcli network ip ipsec sp list**.

Resultados

El host muestra una lista de todas las directivas de seguridad disponibles.

Crear una directiva de seguridad IPsec

Cree una directiva de seguridad para determinar cuándo se debe utilizar el conjunto de parámetros de autenticación y cifrado en una asociación de seguridad. Puede agregar una directiva de seguridad mediante el comando ESXCLI de vSphere CLI.

Requisitos previos

Antes de crear una directiva de seguridad, agregue una asociación de seguridad con los parámetros de autenticación y cifrado adecuados, tal como se describe en Agregar una asociación de seguridad IPsec.

Procedimiento

- En el símbolo del sistema, introduzca el comando **esxcli network ip ipsec sp add** con una o más de las siguientes opciones.

Opción	Descripción
--sp-source= *source address*	Requerido. Especifique la dirección IP de origen y la longitud del prefijo.
--sp-destination= *destination address*	Requerido. Especifique la dirección de destino y la longitud del prefijo.

Opción	Descripción
--source-port= *port*	Requerido. Especifique el puerto de origen. El puerto de origen debe ser un número entre 0 y 65535.
--destination-port= *port*	Requerido. Especifique el puerto de destino. El puerto de origen debe ser un número entre 0 y 65535.
--upper-layer-protocol= *protocol*	Especifique el protocolo de capa superior mediante uno de los siguientes parámetros. ■ `tcp` ■ `udp` ■ `icmp6` ■ `any`
--flow-direction= *direction*	Especifique la dirección en la que desea supervisar el tráfico mediante `in` o `out`.
--action= *action*	Utilice los siguientes parámetros para especificar la acción que se debe realizar cuando se encuentra tráfico con los parámetros especificados. ■ `none`: no realice ninguna acción. ■ `discard`: no permita la entrada o salida de datos. ■ `ipsec`: utilice la información de autenticación y cifrado proporcionada en la asociación de seguridad para determinar si los datos provienen de un origen confiable.
--sp-mode= *mode*	Especifique el modo, ya sea `tunnel` o `transport`.
--sa-name=*security association name*	Requerido. Proporcione el nombre de la asociación de seguridad para la directiva de seguridad que se va a utilizar.
--sp-name=*name*	Requerido. Proporcione un nombre para la directiva de seguridad.

Ejemplo: Nuevo comando de directiva de seguridad

En el siguiente ejemplo se incluyen saltos de línea adicionales para facilitar la lectura.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

Quitar una directiva de seguridad IPsec

Es posible eliminar una directiva de seguridad del host ESXi mediante el comando ESXCLI de vSphere CLI.

Requisitos previos

Compruebe que la directiva de seguridad que desea utilizar no esté en uso. Si intenta eliminar una directiva de seguridad en uso, la operación de eliminación generará errores.

Procedimiento

- En el símbolo del sistema, introduzca el comando **`esxcli network ip ipsec sp remove --sa-name`** ***`security policy name`***.

  Para eliminar todas las directivas de seguridad, introduzca el comando **`esxcli network ip ipsec sp remove --remove-all`**.

Garantizar la correcta configuración de SNMP

Si SNMP no se configura correctamente, puede enviarse información de supervisión a un host malicioso. El host malicioso puede usar esta información para planificar un ataque.

SNMP debe configurarse en cada host ESXi. Puede usar vCLI, PowerCLI o vSphere Web Services SDK para la configuración.

Consulte la publicación de *Supervisión y rendimiento* para obtener información detallada de la instalación de SNMP 3.

Procedimiento

1 Ejecute el siguiente comando para determinar si SNMP se utiliza actualmente.

```
esxcli system snmp get
```

2 Para habilitar SNMP, ejecute el siguiente comando.

```
esxcli system snmp set --enable true
```

3 Para deshabilitar SNMP, ejecute el siguiente comando.

```
esxcli system snmp set --enable false
```

Prácticas recomendadas de seguridad de redes de vSphere

Seguir las prácticas recomendadas de seguridad de redes permite garantizar la integridad de la implementación de vSphere.

Recomendaciones generales sobre seguridad de redes

El primer paso para proteger el entorno de las redes es seguir las recomendaciones generales sobre seguridad de red. A continuación, puede pasar a áreas especiales, como la protección de la red con firewalls o IPsec.

- El protocolo de árbol de expansión (Spanning Tree Protocol, STP) detecta cuándo se van a formar bucles en la topología de la red e impide que suceda. Los conmutadores virtuales de VMware evitan los bucles de otras maneras, pero no admiten el protocolo STP directamente. Cuando se producen cambios en la topología de la red, se necesita un tiempo (entre 30 y 50 segundos) para que la red reconozca la topología. Durante ese tiempo, no se permite que el tráfico pase. Para evitar estos problemas, los proveedores de red han creado funciones para habilitar que los puertos de conmutador sigan reenviando el tráfico. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/kb/1003804. Consulte la documentación del proveedor de red para conocer las configuraciones de red y de hardware de red adecuadas.
- Asegúrese de que el tráfico de Netflow de un conmutador virtual distribuido se envíe solamente a direcciones IP de recopiladores autorizados. Las exportaciones de Netflow no están cifradas y pueden contener información sobre la red virtual. Con esta información aumenta la posibilidad de que los atacantes puedan ver y capturar información confidencial. Si se necesita una exportación de Netflow, compruebe que todas las direcciones IP de destino de Netflow sean correctas.
- Use los controles de acceso basado en funciones para asegurarse de que solo los administradores autorizados tengan acceso a los componentes de redes virtuales. Por ejemplo, se debe otorgar a los administradores de máquinas virtuales acceso solo a los grupos de puertos en los que residen sus máquinas virtuales. Otorgue a los administradores de red acceso a todos los componentes de redes virtuales, pero no acceso a las máquinas virtuales. Si se limita el acceso, se reduce el riesgo de una configuración incorrecta, ya sea accidental o malintencionada, y se aplican los conceptos de seguridad clave de división de tareas y privilegios mínimos.
- Asegúrese de que los grupos de puertos no estén configurados con el valor de la VLAN nativa. A menudo, los conmutadores físicos se configuran con una VLAN nativa y esa VLAN nativa suele ser VLAN 1 de forma predeterminada. ESXi no tiene una VLAN nativa. Las tramas con VLAN especificadas en el grupo de puertos tienen una etiqueta, pero las tramas con VLAN no especificadas en el grupo de puertos no están etiquetadas. Esta situación puede generar un problema porque las máquinas virtuales que se etiquetan con un 1 terminan perteneciendo a una VLAN nativa del conmutador físico.

  Por ejemplo, las tramas de la VLAN 1 de un conmutador físico de Cisco no tienen etiquetas porque la VLAN 1 es la VLAN nativa de ese conmutador físico. No obstante, los marcos del host ESXi que están especificados como VLAN 1 se etiquetan con un 1. Como resultado, el tráfico del host ESXi que está destinado a la VLAN nativa no se enruta correctamente porque está etiquetado con un 1 en lugar de no tener etiqueta. El tráfico del conmutador físico que

viene de la VLAN nativa no es visible porque no está etiquetado. Si el grupo de puertos del conmutador virtual de ESXi usa el identificador de la VLAN nativa, el tráfico proveniente de las máquinas virtuales de ese puerto no será visible para la VLAN nativa del conmutador, ya que este último espera tráfico sin etiquetas.

- Asegúrese de que los grupos de puertos no estén configurados con los valores de la VLAN reservados para los conmutadores físicos ascendentes. Los conmutadores físicos reservan ciertos identificadores de VLAN para fines internos y generalmente no permiten el tráfico configurado con estos valores. Por ejemplo, los conmutadores Cisco Catalyst generalmente reservan las VLAN 1001-1024 y 4094. El uso de una VLAN reservada puede provocar la denegación de servicio en la red.
- Asegúrese de que los grupos de puertos no estén configurados con la VLAN 4095, con excepción del etiquetado de invitado virtual (VGT). Al configurar un grupo de puertos con la VLAN 4095, se activa el modo de VGT. En este modo, el conmutador virtual pasa todas las tramas de red a la máquina virtual sin modificar las etiquetas de la VLAN, y deja que la máquina virtual se encargue de ellas.
- Restrinja las anulaciones de la configuración de nivel de puerto de un conmutador virtual distribuido. Las anulaciones de la configuración de nivel de puerto están deshabilitadas de forma predeterminada. Cuando se habilitan las anulaciones, se puede usar una configuración de seguridad diferente para una máquina virtual y para el nivel de grupo de puertos. Algunas máquinas virtuales requieren una configuración única, pero la supervisión es fundamental. Si las anulaciones no se supervisan, cualquiera que tenga acceso a una máquina virtual con una configuración de conmutador virtual distribuido poco segura puede intentar aprovecharse de dicho acceso.
- Asegúrese de que el tráfico reflejado del conmutador virtual distribuido se envíe solo a los puertos o las VLAN de recopiladores autorizados. vSphere Distributed Switch puede reflejar el tráfico de un puerto a otro para permitir que los dispositivos de captura de paquetes recopilen flujos de tráfico específicos. La funcionalidad de creación de reflejo de puertos envía una copia de todo el tráfico especificado en formato no cifrado. El tráfico reflejado contiene todos los datos en los paquetes capturados, por lo que tales datos pueden verse afectados por completo si se envían a una dirección incorrecta. Si se requiere la creación de reflejo del puerto, verifique que la VLAN de destino del puerto reflejado, el puerto y los identificadores de vínculo superior sean correctos.

Etiquetar componentes de redes

La identificación de los diversos componentes de la arquitectura de redes es esencial y permite garantizar que no se introduzcan errores a medida que se expande la red.

Siga estas prácticas recomendadas:

- Asegúrese de que los grupos de puertos se configuren con una etiqueta de red clara. Estas etiquetas actúan como un descriptor de funciones del grupo de puertos y permiten identificar la función de cada grupo de puertos a medida que se incrementa la complejidad de la red.

- Asegúrese de que cada vSphere Distributed Switch contenga una etiqueta de red clara donde se indique la función o la subred IP de ese conmutador. Esta etiqueta actúa como un descriptor de funciones para el conmutador, al igual que el nombre de host requerido para los conmutadores físicos. Por ejemplo, se puede etiquetar el conmutador como interno para indicar que es para las redes internas. No se puede cambiar la etiqueta de un conmutador virtual estándar.

Documentación y verificación del entorno VLAN de vSphere

Compruebe el entorno de VLAN regularmente para evitar futuros problemas. Documente en detalle el entorno de VLAN y asegúrese de que los identificadores de VLAN se utilicen una sola vez. La documentación puede ayudar a solucionar problemas y resulta fundamental para expandir el entorno.

Procedimiento

1 Asegúrese de que todos los identificadores de vSwitch y VLAN estén documentados detalladamente.

   Si utiliza un etiquetado de VLAN en un conmutador virtual, los identificadores deben coincidir con los identificadores de los conmutadores ascendentes con reconocimiento de VLAN. Si no se hace un seguimiento completo de los identificadores de VLAN, la reutilización de identificadores por error puede producir tráfico entre las máquinas virtuales y físicas inadecuadas. De modo similar, si los identificadores de VLAN son incorrectos o faltan, puede bloquearse el tráfico entre las máquinas físicas y virtuales en los lugares donde el tráfico debiera circular.

2 Compruebe que los identificadores de VLAN de todos los grupos de puertos virtuales distribuidos (instancias dvPortgroup) estén documentados detalladamente.

   Si utiliza un etiquetado de VLAN en un dvPortgroup, los identificadores deben coincidir con los identificador de los conmutadores ascendentes externos con reconocimiento de VLAN. Si no se hace un seguimiento completo de los identificadores de VLAN, la reutilización de identificadores por error puede producir tráfico entre las máquinas virtuales y físicas inadecuadas. De modo similar, si los identificadores de VLAN son incorrectos o faltan, puede bloquearse el tráfico entre las máquinas físicas y virtuales en los lugares donde el tráfico debiera circular.

3 Compruebe que los identificadores de VLAN privada de todos los conmutadores virtuales distribuidos estén documentados detalladamente.

   Las VLAN privadas (PVLAN) de los conmutadores virtuales distribuidos requieren identificadores de VLAN principales y secundarios. Estos identificadores deben coincidir con los identificadores de los conmutadores ascendentes externos con reconocimiento de PVLAN. Si no se hace un seguimiento completo de los identificadores de VLAN, la reutilización

de identificadores por error puede producir tráfico entre las máquinas virtuales y físicas inadecuadas. De modo similar, si los identificadores de PVLAN son incorrectos o faltan, puede bloquearse el tráfico entre las máquinas físicas y virtuales en los lugares donde el tráfico debiera circular.

4 Compruebe que los enlaces troncales de VLAN estén conectados únicamente a los puertos de conmutadores físicos que funcionan como enlaces troncales.

   Cuando conecte un conmutador virtual a un puerto troncal de VLAN, debe configurar correctamente tanto el conmutador virtual como el físico en el puerto de vínculo superior. Si el conmutador físico no está configurado adecuadamente, se reenvían las tramas con el encabezado VLAN 802.1q a un conmutador que no espera esa llegada.

Adoptar prácticas de aislamiento de red

Las prácticas de aislamiento de red refuerzan en gran medida la seguridad de la red en su entorno de vSphere.

Aislar la red de administración

La red de administración de vSphere proporciona acceso a la interfaz de administración de vSphere en cada componente. Los servicios que se ejecutan en la interfaz de administración ofrecen una oportunidad para que un atacante obtenga acceso con privilegios a los sistemas. Los ataques remotos suelen comenzar al obtener acceso a esta red. Si un atacante obtiene acceso a la red de administración, significa que ha dado un gran paso para seguir obteniendo acceso no autorizado.

Para lograr un control estricto del acceso a la red de administración, protéjalo con el nivel de seguridad de la máquina virtual más segura que se ejecuta en un host o clúster de ESXi. Más allá del nivel de restricción que tenga la red de administración, los administradores deben acceder a ella para configurar los hosts ESXi y el sistema vCenter Server.

Coloque el grupo de puertos de administración de vSphere en una VLAN dedicada de un conmutador estándar común. El tráfico (de máquinas virtuales) de producción puede compartir el conmutador estándar si las máquinas virtuales de producción no utilizan la VLAN del grupo de puertos de administración de vSphere.

Compruebe que el segmento de red no esté enrutado, excepto en las redes en las que haya otras entidades relacionadas con la administración. Enrutar un segmento de red podría tener sentido para vSphere Replication. En particular, asegúrese de que el tráfico de las máquinas virtuales de producción no se pueda enrutar a esta red.

Para lograr un control estricto del acceso a la funcionalidad de administración, use uno de los métodos siguientes.

- Para entornos de extrema confidencialidad, configure una puerta de enlace controlada u otro método controlado para acceder a la red de administración. Por ejemplo, requiera que los administradores se conecten a la red de administración a través de una VPN. Conceda acceso a la red de administración solo a los administradores de confianza.

- Configure JumpBoxes que ejecuten clientes de administración.

Aislar el tráfico de almacenamiento

Compruebe que el tráfico de almacenamiento basado en IP esté aislado. El almacenamiento basado en IP incluye iSCSI y NFS. Las máquinas virtuales pueden compartir conmutadores virtuales y VLAN con configuraciones de almacenamiento basadas en IP. Este tipo de configuración puede exponer el tráfico de almacenamiento basado en IP a usuarios de máquinas virtuales no autorizados.

El almacenamiento basado en IP no suele estar cifrado. Cualquier persona que tenga acceso a esta red puede ver el tráfico de almacenamiento basado en IP. Para impedir que usuarios no autorizados vean el tráfico de almacenamiento basado en IP, separe lógicamente el tráfico de red de almacenamiento basado en IP del tráfico de producción. Configure los adaptadores de almacenamiento basado en IP en VLAN distintas o segmentos de red de la red de administración VMkernel para restringir la visualización del tráfico a usuarios no autorizados.

Aislar el tráfico de vMotion

La información de migración de vMotion se transmite en texto sin formato. Cualquiera que tenga acceso a la red puede ver la información que pasa por ella. Los posibles atacantes pueden interceptar el tráfico de vMotion para obtener el contenido de memoria de una máquina virtual. También pueden preparar un ataque de MiTM en el que el contenido se modifica durante la migración.

Separe el tráfico de vMotion del tráfico de producción en una red aislada. Configure la red para que no se pueda enrutar, es decir, asegúrese de que no haya un enrutador de Capa 3 expandiendo esta u otras redes, a fin de restringir el acceso exterior a esta red.

Use una VLAN dedicada en un conmutador estándar común para el grupo de puertos de vMotion. El tráfico (de máquinas virtuales) de producción puede usar el mismo conmutador estándar si las máquinas virtuales de producción no utilizan la VLAN del grupo de puertos de vMotion.

Aislar el tráfico de vSAN

Al configurar la red de vSAN, aísle el tráfico de vSAN en su propio segmento de red de capa 2. Puede realizar este aislamiento mediante conmutadores o puertos dedicados o a través de una VLAN.

Usar conmutadores virtuales con vSphere Network Appliance API solo cuando es necesario

No configure el host para que envíe información de red a una máquina virtual a menos que esté utilizando productos que usan vSphere Network Appliance API (DvFilter). Si vSphere Network Appliance API está habilitado, un atacante puede intentar conectar una máquina virtual al filtro. Esta conexión puede abrir el acceso a la red de otras máquinas virtuales del host.

Si utiliza un producto que usa esta API, compruebe que el host esté configurado correctamente. Consulte las secciones sobre DvFilter en *Desarrollo e implementación de soluciones de vSphere, vServices y agentes de ESX*. Si el host está configurado para usar la API, compruebe que el valor del parámetro `Net.DVFilterBindIpAddress` coincida con el producto que usa la API.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, haga clic en **Configuración avanzada del sistema**.

4 Desplácese hacia abajo hasta `Net.DVFilterBindIpAddress` y compruebe que el parámetro tenga un valor vacío.

  El orden de los parámetros no es estrictamente alfabético. Escriba **`DvFilter`** en el cuadro de texto “Filtrar” para mostrar todos los parámetros relacionados.

5 Compruebe la configuración.

  - Si no utiliza la configuración de DvFilter, asegúrese de que el valor esté en blanco.
  - Si está utilizando la configuración de DvFilter, asegúrese de que el valor del parámetro sea correcto. El valor debe coincidir con el valor del producto que usa el DvFilter.

Prácticas recomendadas relacionadas con varios componentes de vSphere

11

Algunas prácticas recomendadas de seguridad, como la configuración de NTP en el entorno, tienen efecto en más de un componente de vSphere. Tenga en cuenta estas recomendaciones al configurar el entorno.

Consulte Capítulo 3 Proteger hosts ESXi y Capítulo 5 Proteger máquinas virtuales para obtener información relacionada.

Este capítulo incluye los siguientes temas:

- Sincronizar los relojes en la red de vSphere
- Prácticas recomendadas de seguridad de almacenamiento
- Comprobar que está deshabilitado el envío de datos de rendimiento del host a los invitados
- Configurar tiempos de espera de ESXi Shell y vSphere Web Client

Sincronizar los relojes en la red de vSphere

Compruebe que todos los componentes de la red de vSphere tengan sus relojes sincronizados. Si los relojes en las máquinas físicas de la red de vSphere no están sincronizados, los certificados SSL y los tokens SAML, que están sujetos a limitaciones temporales, pueden no reconocerse como válidos en las comunicaciones entre máquinas de la red.

Los relojes que no están sincronizados pueden ocasionar problemas de autenticación que, a su vez, pueden provocar errores en la instalación o evitar que se inicie el servicio `vmware-vpxd` de vCenter Server Appliance.

Las incoherencias de hora en vSphere pueden provocar un error en el primer arranque de los diferentes servicios según la ubicación en el entorno donde la hora no sea precisa y el momento en el que se sincronice la hora. Normalmente, los problemas se producen cuando el host ESXi de destino para el dispositivo vCenter Server Appliance de destino no está sincronizado con NTP. De forma similar, se pueden presentar problemas si el dispositivo vCenter Server Appliance de destino se migra a un host ESXi establecido en otra hora debido a un DRS completamente automatizado.

Para evitar problemas de sincronización de hora, asegúrese de que lo siguiente sea correcto antes de instalar, migrar o actualizar un dispositivo vCenter Server Appliance.

- El host ESXi de destino donde se desea implementar el dispositivo vCenter Server Appliance de destino está sincronizado con NTP.
- El host ESXi donde se ejecuta el dispositivo vCenter Server Appliance de origen está sincronizado con NTP.
- Al actualizar o migrar, si el dispositivo vCenter Server Appliance está conectado a una instancia externa de Platform Services Controller, asegúrese de que el host ESXi donde se ejecuta la instancia externa de Platform Services Controller esté sincronizado con NTP.
- Si desea realizar una actualización o una migración, compruebe que la instancia de vCenter Server o vCenter Server Appliance de origen y la instancia externa de Platform Services Controller tengan la hora correcta.

Verifique que todos los equipos host de Windows en los que se ejecuta vCenter Server estén sincronizados con el servidor de tiempo de red (NTP). Consulte el artículo KB 1318 de la base de conocimientos.

Para sincronizar los relojes de ESXi con un servidor NTP, puede usar VMware Host Client.
Para obtener información sobre cómo editar la configuración de hora de un host ESXi, consulte *Administrar un host único de vSphere*.

Para obtener información sobre cómo cambiar la configuración de sincronización de hora de vCenter Server Appliance, consulte "Configurar los ajustes de sincronización de hora en vCenter Server Appliance" en *Configuración de vCenter Server Appliance*.

Para obtener información sobre cómo editar la configuración de hora de un host, consulte "Editar la configuración de hora para un host" en *Administrar vCenter Server y hosts*.

- Sincronización de los relojes de ESXi con un servidor horario de red

  Antes de instalar vCenter Server o de implementar vCenter Server Appliance, asegúrese de que todas las máquinas de la red de vSphere tengan los relojes sincronizados.

- Configurar la sincronización de hora en vCenter Server Appliance

  Puede cambiar la configuración de hora en vCenter Server Appliance tras la implementación.

Sincronización de los relojes de ESXi con un servidor horario de red

Antes de instalar vCenter Server o de implementar vCenter Server Appliance, asegúrese de que todas las máquinas de la red de vSphere tengan los relojes sincronizados.

Esta tarea explica cómo configurar NTP desde VMware Host Client. Se puede utilizar en su lugar el comando de vCLI `vicfg-ntp`. Consulte la *referencia de vSphere Command-Line Interface*.

Procedimiento

1 Inicie VMware Host Client y conéctese al host ESXi.

2 Haga clic en **Administrar**.

3 En **Sistema**, haga clic en **Hora y fecha** y, a continuación, en **Editar configuración**.

4 Seleccione **Usar protocolo de hora de red (Habilitar el cliente NTP)**.

5 En el cuadro de texto Servidores NTP, introduzca la dirección IP o el nombre de dominio completo de uno o más servidores NTP con los que se realizará la sincronización.

6 (opcional) Establezca la directiva de inicio y el estado de servicio.

7 Haga clic en **Guardar**.

   El host se sincroniza con el servidor NTP.

Configurar la sincronización de hora en vCenter Server Appliance

Puede cambiar la configuración de hora en vCenter Server Appliance tras la implementación.

Cuando implementa vCenter Server Appliance, puede decidir que el método de sincronización de hora sea mediante un servidor NTP o a través de VMware Tools. En caso de que la configuración de hora de la red de vSphere cambie, puede editar vCenter Server Appliance y configurar la sincronización horaria mediante los comandos del shell del dispositivo.

Cuando habilita la sincronización horaria periódica, VMware Tools configura la hora del sistema operativo invitado para que sea la misma que la hora del host.

Una vez que se sincroniza la hora, VMware Tools comprueba cada un minuto si los relojes del sistema operativo invitado y el host aún coinciden. Si no lo hacen, el reloj del sistema operativo invitado se sincroniza para que coincida con el reloj del host.

El software de sincronización de hora nativo, como el protocolo de hora de red (NTP), suele ser más preciso que la sincronización horaria periódica de VMware Tools y, por lo tanto, es el método preferido. En vCenter Server Appliance, solo puede utilizar un modo de sincronización horaria periódica. Si decide utilizar software de sincronización de hora nativo, se desactiva la sincronización horaria periódica de VMware Tools en vCenter Server Appliance, y viceversa.

Usar la sincronización de hora de VMware Tools

Puede configurar vCenter Server Appliance para utilizar la sincronización de hora de VMware Tools.

Procedimiento

1 Acceda al shell del dispositivo e inicie sesión como usuario que tiene la función de administrador o superadministrador.

   El usuario predeterminado con la función de superadministrador es root.

2 Ejecute el comando para habilitar la sincronización de hora de VMware Tools.

```
timesync.set --mode host
```

3 (opcional) Ejecute el comando para comprobar que la sincronización de hora de VMware Tools se aplicó correctamente.

```
timesync.get
```

El comando devuelve un mensaje donde se indica que la sincronización de hora se encuentra en el modo host.

Resultados

La hora del dispositivo se sincroniza con la hora del host ESXi.

Agregar o reemplazar servidores NTP en la configuración de vCenter Server Appliance

Para configurar vCenter Server Appliance de modo que utilice la sincronización de hora basada en NTP, debe agregar los servidores NTP a la configuración de vCenter Server Appliance.

Procedimiento

1 Acceda al shell del dispositivo e inicie sesión como usuario que tiene la función de administrador o superadministrador.

   El usuario predeterminado con la función de superadministrador es root.

2 Agregue servidores NTP a la configuración de vCenter Server Appliance mediante la ejecución del comando `ntp.server.add`.

   Por ejemplo, ejecute el siguiente comando:

```
ntp.server.add --servers IP-addresses-or-host-names
```

   Aquí, *IP-addresses-or-host-names* es una lista separada por comas de direcciones IP o nombres de host de los servidores NTP.

   Este comando agrega servidores NTP a la configuración. Si la sincronización de hora se basa en un servidor NTP, el daemon de NTP se reinicia para volver a cargar los nuevos servidores NTP. De lo contrario, este comando solo agrega los nuevos servidores NTP a la configuración de NTP existente.

3 (opcional) Para eliminar servidores NTP antiguos y agregar nuevos a la configuración de vCenter Server Appliance, ejecute el comando `ntp.server.set`.

   Por ejemplo, ejecute el siguiente comando:

```
ntp.server.set --servers IP-addresses-or-host-names
```

   Aquí, *IP-addresses-or-host-names* es una lista separada por comas de direcciones IP o nombres de host de los servidores NTP.

Este comando elimina servidores NTP antiguos de la configuración y establece los servidores NTP de entrada. Si la sincronización de hora se basa en un servidor NTP, el daemon de NTP se reinicia para volver a cargar la nueva configuración de NTP. De lo contrario, este comando solo reemplaza los servidores de la configuración de NTP por los servidores que proporciona como entrada.

4 (opcional) Ejecute el comando para comprobar que se aplicó correctamente la nueva configuración de NTP.

```
ntp.get
```

El comando devuelve una lista separada con espacios de los servidores configurados para la sincronización de NTP. Si la sincronización de NTP está habilitada, el comando informa de que el estado de la configuración de NTP es Activado. Si la sincronización de NTP está deshabilitada, el comando informa de que el estado de la configuración de NTP es Desactivado.

Pasos siguientes

Si la sincronización de NTP está deshabilitada, se puede configurar la sincronización de hora en vCenter Server Appliance para que se base en un servidor NTP. Consulte Sincronizar la hora de vCenter Server Appliance con un servidor NTP.

Sincronizar la hora de vCenter Server Appliance con un servidor NTP

Puede configurar la sincronización de hora en vCenter Server Appliance para que se base en un servidor NTP.

Requisitos previos

Establezca uno o más servidores Network Time Protocol (NTP) en la configuración de vCenter Server Appliance. Consulte Agregar o reemplazar servidores NTP en la configuración de vCenter Server Appliance.

Procedimiento

1 Acceda al shell del dispositivo e inicie sesión como usuario que tiene la función de administrador o superadministrador.

El usuario predeterminado con la función de superadministrador es root.

2 Ejecute el comando para habilitar la sincronización de hora basada en NTP.

```
timesync.set --mode NTP
```

3 (opcional) Ejecute el comando para comprobar que se aplicó correctamente la sincronización de NTP.

```
timesync.get
```

El comando devuelve que la sincronización de hora se encuentra en el modo NTP.

Prácticas recomendadas de seguridad de almacenamiento

Siga las prácticas recomendadas de seguridad de almacenamiento que indica su proveedor de seguridad de almacenamiento. También puede aprovechar CHAP y Mutual CHAP para proteger el almacenamiento iSCSI, crear máscaras para los recursos de SAN y dividirlos en zonas, y configurar credenciales Kerberos para NFS 4.1.

Consulte además la documentación de *Administrar VMware vSAN*.

Proteger almacenamiento iSCSI

El almacenamiento que se configura en un host puede incluir una o más redes de área de almacenamiento (SAN) que utilizan iSCSI. Cuando se configura iSCSI en un host, se pueden tomar medidas para minimizar los riesgos de seguridad.

iSCSI admite el acceso a los dispositivos SCSI y el intercambio de datos mediante TCP/IP en un puerto de red en lugar de hacerlo a través de una conexión directa con el dispositivo SCSI. Una transacción de iSCSI encapsula bloques de datos SCSI sin formato en registros iSCSI y transmite los datos al dispositivo o el usuario que los solicite.

Las SAN iSCSI admiten el uso eficaz de la infraestructura Ethernet existente para proporcionar acceso a los hosts a los recursos de almacenamiento que pueden compartir dinámicamente. Las SAN iSCSI son una solución de almacenamiento económica para los entornos que dependen de un grupo de almacenamiento común para varios usuarios. Al igual que con cualquier sistema en red, la seguridad de las SAN iSCSI puede verse comprometida debido a infracciones.

Nota Los requisitos y procedimientos para proteger la SAN iSCSI son similares para los adaptadores iSCSI de hardware asociados a los hosts y para iSCSI configurado directamente mediante el host.

Proteger dispositivos de iSCSI

Para proteger los dispositivos de iSCSI, es necesario que el host ESXi o el iniciador puedan autenticarse en el dispositivo de iSCSI o en el destino, siempre que el host intente acceder a datos del LUN de destino.

La autenticación garantiza que el iniciador tenga derecho a acceder a un destino. Conceda este derecho al configurar la autenticación en el dispositivo de iSCSI.

ESXi no admite el protocolo Secure Remote Protocol (SRP) o los métodos de autenticación de clave pública de iSCSI. Kerberos se puede utilizar solo con NFS 4.1.

ESXi admite la autenticación de CHAP y Mutual CHAP. En el documento *Almacenamiento de vSphere* se explica cómo seleccionar el mejor método de autenticación para el dispositivo de iSCSI y cómo configurar CHAP.

Asegúrese de que las contraseñas de CHAP sean únicas. Configure un secreto de autenticación mutua diferente para cada host. Si es posible, configure un secreto diferente para cada cliente que se conecte al host ESXi. Los secretos exclusivos aseguran que un atacante no pueda crear otro host arbitrario y autenticarse en el dispositivo de almacenamiento, incluso si hay un host está en riesgo. Si hay una contraseña compartida y un host comprometido, un atacante podría autenticarse en el dispositivo de almacenamiento.

Proteger una SAN iSCSI

Al planificar la configuración de iSCSI, tome las medidas necesarias para mejorar la seguridad general de la SAN iSCSI. La configuración de iSCSI es tan segura como la red IP, por lo tanto, si aplica estándares de seguridad adecuados al configurar la red, ayuda a proteger el almacenamiento iSCSI.

A continuación, se presentan sugerencias específicas para aplicar estándares de seguridad adecuados.

Proteger datos transmitidos

Uno de los principales riesgos en las SAN iSCSI es que un atacante puede capturar los datos de almacenamiento transmitidos.

Tome medidas adicionales para evitar que los atacantes vean datos de iSCSI con facilidad. Ni el adaptador de iSCSI de hardware ni el iniciador iSCSI de ESXi cifran los datos que transmiten hacia y desde los destinos, lo que hace que los datos sean más vulnerables a ataques de analizadores de protocolos (sniffer).

Si permite que las máquinas virtuales compartan conmutadores estándar y VLAN con la configuración de iSCSI, se corre el riesgo de que algún atacante de máquinas virtuales haga un uso incorrecto del tráfico iSCSI. Para ayudar a garantizar que los intrusos no puedan escuchar transmisiones de iSCSI, asegúrese de que ninguna de las máquinas virtuales pueda ver la red de almacenamiento iSCSI.

Si usa un adaptador de iSCSI de hardware, puede lograr esto comprobando que el adaptador de iSCSI y el adaptador físico de red de ESXi no se conecten accidentalmente fuera del host debido al uso compartido de un conmutador o a algún otro motivo. Si configura iSCSI directamente mediante el host ESXi, podrá lograr esto configurando el almacenamiento iSCSI con un conmutador estándar diferente al que se usa en las máquinas virtuales.

Además de proteger la SAN iSCSI con un conmutador estándar dedicado, puede configurar la SAN iSCSI en su propia VLAN para mejorar el rendimiento y la seguridad. Al colocar la configuración de iSCSI en una VLAN distinta, se garantiza que ningún dispositivo que no sea el adaptador de iSCSI pueda ver transmisiones dentro de la SAN iSCSI. Además, la congestión de la red desde otros orígenes no puede interferir en el tráfico iSCSI.

Proteger los puertos de iSCSI

Al utilizar dispositivos de iSCSI, ESXi no abre ningún puerto que escuche conexiones de red. Esta medida reduce la posibilidad de que un intruso logre entrar a ESXi por los puertos de reserva y tome el control del host. De esta manera, la ejecución de iSCSI no presenta ningún riesgo adicional de seguridad al final de la conexión de ESXi.

Todos los dispositivos de destino iSCSI que se utilicen deben tener uno o más puertos TCP abiertos para escuchar las conexiones de iSCSI. Si existe alguna vulnerabilidad de seguridad en el software del dispositivo iSCSI, los datos pueden estar en riesgo incluso si ESXi funciona correctamente. Para reducir este riesgo, instale todas las revisiones de seguridad que le proporcione el fabricante del equipo de almacenamiento y limite los dispositivos conectados a la red de iSCSI.

Crear máscaras y dividir en zonas para recursos de SAN

Puede utilizar la división en zonas y el enmascaramiento de LUN para segregar la actividad de SAN y restringir el acceso a los dispositivos de almacenamiento.

Puede proteger el acceso al almacenamiento en el entorno de vSphere mediante la división en zonas y el enmascaramiento de LUN con los recursos de SAN. Por ejemplo, puede administrar zonas definidas para pruebas de manera independiente en la SAN para que no interfieran con la actividad de las zonas de producción. De forma similar, puede configurar diferentes zonas para distintos departamentos.

Al configurar zonas, tenga en cuenta los grupos de hosts que estén configurados en el dispositivo SAN.

Las capacidades de división en zonas y de máscaras para cada conmutador SAN y matriz de disco, junto con las herramientas de administración de enmascaramiento de LUN, son específicas del proveedor.

Consulte la documentación del proveedor de SAN y la documentación de *Almacenamiento de vSphere*.

Usar Kerberos para NFS 4.1

Con la versión 4.1 de NFS, ESXi admite el mecanismo de autenticación Kerberos.

El mecanismo RPCSEC_GSS Kerberos es un servicio de autenticación. Permite instalar un cliente de NFS 4.1 en ESXi para probar su identidad en un servidor NFS antes de montar un recurso compartido de NFS. La seguridad Kerberos utiliza criptografía para funcionar en una conexión de red no segura.

La implementación de ESXi de Kerberos para NFS 4.1 proporciona dos modelos de seguridad, krb5 y krb5i, que ofrecen distintos niveles de seguridad.

- Kerberos para autenticación solamente (krb5) admite la comprobación de identidad.

- Kerberos para autenticación e integridad de datos (krb5i), además de la comprobación de identidad, proporciona servicios de integridad de datos. Estos servicios ayudan a proteger el tráfico de NFS para evitar la alteración mediante la comprobación de posibles modificaciones en los paquetes de datos.

Kerberos admite algoritmos de cifrado que evitan que los usuarios no autorizados puedan acceder al tráfico de NFS. El cliente NFS 4.1 en ESXi intenta usar el algoritmo AES256-CTS-HMAC-SHA1-96 o AES128-CTS-HMAC-SHA1-96 para acceder a un recurso compartido en el servidor NAS. Antes de utilizar los almacenes de datos de NFS 4.1, asegúrese de que AES256-CTS-HMAC-SHA1-96 o AES128-CTS-HMAC-SHA1-96 estén habilitados en el servidor NAS.

En la siguiente tabla, se comparan los niveles de seguridad de Kerberos admitidos por ESXi.

Tabla 11-1. Tipos de seguridad de Kerberos

		ESXi 6.0	**ESXi 6.5 y versiones posteriores**
Kerberos para autenticación solamente (krb5)	Suma de comprobación de integridad para encabezado RPC	Sí con DES	Sí con AES
	Comprobación de integridad para datos de RPC	No	No
Kerberos para autenticación e integridad de datos (krb5i)	Suma de comprobación de integridad para encabezado RPC	Sin krb5i	Sí con AES
	Comprobación de integridad para datos de RPC		Sí con AES

Al utilizar la autenticación Kerberos, se deben tener en cuenta las siguientes consideraciones:

- ESXi utiliza Kerberos con el dominio de Active Directory.
- Como administrador de vSphere, debe especificar credenciales de Active Directory para proporcionar acceso a un usuario de NFS a los almacenes de datos Kerberos de NFS 4.1. Se utiliza un único conjunto de credenciales para acceder a todos los almacenes de datos Kerberos montados en ese host.
- Cuando varios hosts ESXi comparten el almacén de datos NFS 4.1, se deben utilizar las mismas credenciales de Active Directory para todos los hosts que tienen acceso al almacén de datos compartido. Para automatizar el proceso de asignación, establezca el usuario en los perfiles de host y aplique el perfil a todos los hosts ESXi.
- No se pueden usar dos mecanismos de seguridad, AUTH_SYS y Kerberos, para el mismo almacén de datos NFS 4.1 compartido por varios hosts.

Consulte la documentación de *Almacenamiento de vSphere* para obtener instrucciones paso a paso.

Comprobar que está deshabilitado el envío de datos de rendimiento del host a los invitados

vSphere incluye contadores de rendimiento de las máquinas virtuales en los sistemas operativos Windows con VMware Tools instalado. Los contadores de rendimiento permiten que los propietarios de las máquinas virtuales realicen análisis precisos del rendimiento en el sistema operativo invitado. De forma predeterminada, vSphere no expone la información del host a la máquina virtual invitada.

De forma predeterminada, la capacidad para enviar datos de rendimiento del host a una máquina virtual está deshabilitada. Esta configuración predeterminada impide que una máquina virtual obtenga información detallada sobre el host físico. Si se produce una infracción de seguridad de la máquina virtual, la configuración no pone a disposición del atacante los datos del host.

Nota El procedimiento siguiente muestra el proceso básico. Considere la posibilidad de usar una de las interfaces de línea de comandos de vSphere (vCLI, PowerCLI, entre otras) para realizar esta tarea simultáneamente en todos los hosts.

Procedimiento

1 En el sistema ESXi que aloja a la máquina virtual, desplácese hasta el archivo VMX.

   Los archivos de configuración de la máquina virtual están ubicados en el directorio `/vmfs/volumes/`*`datastore`*, donde *datastore* corresponde al nombre del dispositivo de almacenamiento en el que están almacenados los archivos de la máquina virtual.

2 En el archivo VMX, compruebe que se haya establecido el siguiente parámetro.

   ```
   tools.guestlib.enableHostInfo=FALSE
   ```

3 Guarde y cierre el archivo.

Resultados

No se puede recuperar la información de rendimiento del host desde la máquina virtual invitada.

Configurar tiempos de espera de ESXi Shell y vSphere Web Client

Para evitar que los intrusos utilicen una sesión inactiva, asegúrese de configurar tiempos de espera para ESXi Shell y vSphere Web Client.

Tiempo de espera de ESXi Shell

Para ESXi Shell, puede establecer los siguientes tiempos de espera desde vSphere Web Client y la interfaz de usuario de la consola directa (DCUI).

Tiempo de espera de disponibilidad

La configuración de tiempo de espera de disponibilidad corresponde a la cantidad de tiempo que puede transcurrir antes de que pueda iniciar sesión tras la habilitación de ESXi Shell. Una vez que transcurre el período de espera, el servicio se deshabilita y los usuarios no pueden iniciar sesión.

Tiempo de espera de inactividad

El tiempo de espera de inactividad corresponde a la cantidad de tiempo que puede transcurrir antes de que se cierren las sesiones interactivas inactivas. Los cambios en el tiempo de espera de inactividad se aplican la próxima vez que un usuario inicia sesión en ESXi Shell. Los cambios no afectan a las sesiones existentes.

Tiempo de espera de vSphere Web Client

De forma predeterminada, las sesiones de vSphere Web Client finalizan después de 120 minutos. Puede cambiar este valor predeterminado en el archivo `webclient.properties`, tal como se indica en la documentación de *Administrar vCenter Server y hosts*.

Administración de la configuración del protocolo TLS con la utilidad de configuración de TLS

12

A partir de vSphere 6.7, solo TLS 1.2 está habilitado de forma predeterminada. TLS 1.0 y TLS 1.1 están deshabilitados de forma predeterminada. Independientemente de que se realicen una instalación nueva, una actualización o una migración, vSphere 6.7 deshabilita TLS 1.0 y TLS 1.1. Es posible usar la utilidad de configuración de TLS para habilitar temporalmente las versiones anteriores del protocolo en los sistemas vSphere 6.7. Una vez que todas las conexiones utilicen TLS 1.2, podrá deshabilitar las versiones anteriores menos seguras.

Nota A partir de vSphere 6.7, la utilidad de configuración de TLS se incluye en el producto. Por lo tanto, ya no se descarga por separado.

Antes de realizar una reconfiguración, conozca su entorno. Según los requisitos del entorno y las versiones de software, es posible que deba volver a habilitar TLS 1.0 y TLS 1.1, además de TLS 1.2, para mantener la interoperabilidad. Para los productos de VMware, consulte el artículo 2145796 de la base de conocimientos de VMware para obtener una lista de los productos de VMware que admiten TLS 1.2. Para la integración con terceros, consulte la documentación del proveedor.

Este capítulo incluye los siguientes temas:

- Puertos que permiten deshabilitar versiones de TLS
- Habilitar o deshabilitar versiones de TLS en vSphere
- Copia de seguridad manual opcional
- Habilitar o deshabilitar versiones de TLS en sistemas de vCenter Server
- Habilitar o deshabilitar versiones de TLS en hosts ESXi
- Habilitar o deshabilitar versiones de TLS en sistemas Platform Services Controller externos
- Buscar protocolos TLS habilitados en vCenter Server
- Revertir los cambios de configuración de TLS
- Habilitar o deshabilitar las versiones de TLS en vSphere Update Manager en Windows

Puertos que permiten deshabilitar versiones de TLS

Cuando se ejecuta la utilidad de configuración de TLS en el entorno de vSphere, se puede deshabilitar TLS en los puertos que usan TLS en los hosts vCenter Server, Platform Services Controller y ESXi. Es posible deshabilitar TLS 1.0, o bien TLS 1.0 y TLS 1.1.

vCenter Server y ESXi utilizan puertos que pueden habilitarse o deshabilitarse para los protocolos TLS. La opción de escaneado de la utilidad de configuración de TLS muestra qué versiones de TLS están habilitadas para cada servicio. Consulte Buscar protocolos TLS habilitados en vCenter Server.

Para obtener la lista de todos los puertos y protocolos compatibles en los productos de VMware, incluidos vSphere y vSAN, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/. Puede buscar puertos por producto de VMware, crear una lista de puertos personalizada e imprimir o guardar listas de puertos.

Notas y advertencias

- Solo puede volver a configurar los siguientes servicios en vCenter Server Appliance.
  - VMware Syslog Collector
  - Interfaz de VMware Appliance Management
  - Servicio de vSphere Update Manager
- En vCenter Server en Windows, si quiere volver a configurar TLS para los puertos de Update Manager, debe editar los archivos de configuración. Consulte Habilitar o deshabilitar las versiones de TLS en vSphere Update Manager en Windows.
- A partir de vSphere 6.7, puede usar TLS 1.2 para cifrar la conexión entre vCenter Server y una instancia externa de Microsoft SQL Server. No se puede utilizar una conexión solo de TLS 1.2 para una base de datos de Oracle externa. Consulte el artículo 2149745 de la base de conocimientos de VMware.
- No deshabilite TLS 1.0 en una instancia de vCenter Server o de Platform Services Controller que se ejecute en Windows Server 2008. Windows 2008 admite únicamente TLS 1.0. Consulte el artículo de Microsoft TechNet *Configuración de TLS/SSL* incluido en la *guía de tecnologías y funciones de servidor*.
- Si cambia los protocolos TLS, debe reiniciar el host ESXi para aplicar los cambios. Debe reiniciar el host incluso si aplica los cambios a través de la configuración del clúster mediante el uso de perfiles de host. Puede reiniciar el host de forma inmediata o aplazar el reinicio para un momento más oportuno.

Habilitar o deshabilitar versiones de TLS en vSphere

Deshabilitar las versiones de TLS es un proceso de varias etapas. Al deshabilitar las versiones de TLS en el orden correcto, se garantiza que el entorno permanezca activo y en ejecución durante el proceso.

1. Si el entorno incluye vSphere Update Manager en Windows y vSphere Update Manager se encuentra en un sistema independiente, deshabilite los protocolos explícitamente mediante la edición de los archivos de configuración. Consulte Habilitar o deshabilitar las versiones de TLS en vSphere Update Manager en Windows.

   vSphere Update Manager en vCenter Server Appliance siempre se incluye con el sistema vCenter Server y el script actualiza el puerto correspondiente.

2. Ejecute la utilidad en vCenter Server.
3. Ejecute la utilidad en cada host ESXi que se administra mediante vCenter Server. Puede realizar esta tarea para cada host o para todos los hosts de un clúster.
4. Si el entorno utiliza una o varias instancias de Platform Services Controller, ejecute la utilidad en cada instancia.

Requisitos previos

Tiene dos opciones para el uso de TLS en su entorno.

- Deshabilite TLS 1.0, y habilite TLS 1.1 y TLS 1.2.
- Deshabilite TLS 1.0 y TLS 1.1, y habilite TLS 1.2.

Copia de seguridad manual opcional

La utilidad de configuración de TLS realiza una copia de seguridad cada vez que el script modifica vCenter Server, Platform Services Controller o vSphere Update Manager en el vCenter Server Appliance. Si necesita una copia de seguridad en un directorio específico, puede realizar una copia de seguridad manual.

No se admite la copia de seguridad de la configuración de ESXi.

Para vCenter Server o Platform Services Controller, el directorio predeterminado es diferente para Windows y el dispositivo.

Sistema operativo	Directorio de copia de seguridad
Windows	`c:\users\`*`current_user`*`\appdata\local\temp\`*`yearmonthdayTtime`*
Linux	`/tmp/`*`yearmonthdayTtime`*

Procedimiento

1 Cambie el directorio a `VcTlsReconfigurator`.

Sistema operativo	Comando
Windows	`cd %VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator`
Linux	`cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`

2 Para realizar una copia de seguridad en un directorio específico, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	*directory_path*`\VcTlsReconfigurator> reconfigureVc backup -d` *backup_directory_path*
Linux	*directory_path*`/VcTlsReconfigurator> ./reconfigureVc backup -d` *backup_directory_path*

3 Compruebe que la copia de seguridad se haya realizado correctamente.

Una copia de seguridad correcta es similar al siguiente ejemplo. El orden en el que se muestran los servicios puede ser diferente cada vez que se ejecuta el comando `reconfigureVc backup` debido a la manera en la que este se ejecuta.

```
vCenter Transport Layer Security reconfigurator, version=6.7.0, build=8070195
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "/var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log".
================= Backing up vCenter Server TLS configuration ==================
Using backup directory: /tmp/20180422T224804
Backing up: vmware-sps
Backing up: vmdird
Backing up: vmware-rbd-watchdog
Backing up: vmware-vpxd
Backing up: vmware-updatemgr
Backing up: vmcam
Backing up: vsphere-client
Backing up: vami-lighttp
Backing up: rsyslog
Backing up: vmware-rhttpproxy
Backing up: vmware-stsd
```

4 (opcional) Si debe realizar una restauración más adelante, puede ejecutar el siguiente comando.

```
reconfigureVc restore -d optional_custom_backup_directory_path
```

Habilitar o deshabilitar versiones de TLS en sistemas de vCenter Server

Puede usar la utilidad de configuración de TLS para habilitar o deshabilitar las versiones de TLS en los sistemas vCenter Server con una instancia externa de Platform Services Controller y en los sistemas vCenter Server con una instancia integrada de Platform Services Controller. Como parte del proceso, puede inhabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2. O bien, puede deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2.

Requisitos previos

Asegúrese de que los hosts y los servicios que administra vCenter Server puedan comunicarse con una versión de TLS que permanezca habilitada. Para los productos que se comunican solo mediante TLS 1.0, la conectividad deja de estar disponible.

Procedimiento

1 Inicie sesión en el sistema de vCenter Server con el nombre de usuario y la contraseña de administrator@vsphere.local, o como otro miembro del grupo de administradores de vCenter Single Sign-On que pueden ejecutar scripts.

2 Desplácese hasta el directorio en donde se encuentra el script.

Sistema operativo	Comando
Windows	`cd %VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator`
Linux	`cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`

3 Ejecute el comando, según su sistema operativo y la versión de TLS que desee utilizar.

- Para deshabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	*directory_path*`\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2`
Linux	*directory_path*`/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2`

- Para deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	*directory_path*`\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2`
Linux	*directory_path*`/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2`

4 Si el entorno incluye otros sistemas vCenter Server, repita el proceso en cada sistema vCenter Server.

5 Repita la configuración en cada host ESXi y en cada instancia de Platform Services Controller.

Habilitar o deshabilitar versiones de TLS en hosts ESXi

Puede usar la utilidad de configuración de TLS para habilitar o deshabilitar las versiones de TLS en un host ESXi. Como parte del proceso, puede inhabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2. O bien, puede deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2.

Para los hosts ESXi, se usa una utilidad diferente que para los demás componentes del entorno de vSphere. La utilidad es específica de la versión y no se puede usar en una versión anterior.

Puede escribir un script para configurar varios hosts.

Requisitos previos

Asegúrese de que los productos o los servicios asociados con el host ESXi puedan comunicarse con TLS 1.1 o TLS 1.2. Para los productos que se comunican solo mediante TLS 1.0, se pierde la conectividad.

Procedimiento

1 Inicie sesión en el sistema de vCenter Server con el nombre de usuario y la contraseña del usuario de vCenter Single Sign-On que puede ejecutar scripts.

2 Desplácese hasta el directorio en donde se encuentra el script.

Sistema operativo	Comando
Windows	`cd %VMWARE_CIS_HOME%\TlsReconfigurator\EsxTlsReconfigurator`
Linux	`cd /usr/lib/vmware-TlsReconfigurator/EsxTlsReconfigurator`

3 En un host ESXi que forma parte de un clúster, ejecute uno de los siguientes comandos.

- Para deshabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2 en todos los hosts de un clúster, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	`reconfigureEsx vCenterCluster -c` *`Cluster_Name`* `-u` *`Administrative_User`* `-p TLSv1.1 TLSv1.2`
Linux	`./reconfigureEsx vCenterCluster -c` *`Cluster_Name`* `-u` *`Administrative_User`* `-p TLSv1.1 TLSv1.2`

- Para deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2 en todos los hosts de un clúster, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	`reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2`
Linux	`./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2`

4 Para un host individual que no forma parte de un clúster, ejecute uno de los siguientes comandos.

- Para deshabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2 en un host individual, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	`reconfigureEsx vCenterHost -h ESXi_Host_Name -u Administrative_User -p TLSv1.1 TLSv1.2`
Linux	`./reconfigureEsx vCenterHost -h ESXi_Host_Name -u Administrative_User -p TLSv1.1 TLSv1.2`

- Para deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2 en un host individual, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	`reconfigureEsx vCenterHost -h` *`ESXi_Host_Name`* `-u` *`Administrative_User`* `-p TLSv1.2`
Linux	`./reconfigureEsx vCenterHost -h` *`ESXi_Host_Name`* `-u` *`Administrative_User`* `-p TLSv1.2`

Nota Para volver a configurar un host ESXi independiente, inicie sesión en un sistema vCenter Server y ejecute el comando `reconfigureEsx` con las opciones `ESXiHost -h` *HOST* `-u` *ESXi_ USER*. En la opción *HOST*, puede especificar la dirección IP o el FQDN de un solo host ESXi o una lista de direcciones IP de host o varios FQDN. Por ejemplo, al iniciar sesión en vCenter Server y ejecutar el siguiente comando, se habilita TLS 1.1 y TLS 1.2 en dos hosts ESXi:

```
./reconfigureEsx ESXiHost -h 198.51.100.2 198.51.100.3 -u root -p TLSv1.1 TLSv1.2
```

Como alternativa, para volver a configurar un host ESXi independiente, puede iniciar sesión en el host y modificar la configuración avanzada de `UserVars.ESXiVPsDisabledProtocols`. Consulte el tema titulado "Configurar opciones de clave TLS/SSL avanzadas" en la documentación de *Administrar un host único de vSphere: VMware Host Client* para obtener más información.

5 Reinicie el host ESXi para completar los cambios del protocolo TLS.

Habilitar o deshabilitar versiones de TLS en sistemas Platform Services Controller externos

Si el entorno incluye uno o varios sistemas Platform Services Controller, puede usar la utilidad de configuración de TLS para cambiar las versiones de TLS que deben admitirse.

Si el entorno utiliza solo una instancia integrada de Platform Services Controller, completó esta tarea anteriormente durante el proceso de vCenter Server. Consulte Habilitar o deshabilitar versiones de TLS en sistemas de vCenter Server.

Nota Continúe con esta tarea solo después de confirmar que cada sistema vCenter Server ejecuta una versión compatible de TLS.

Como parte del proceso, puede inhabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2. O bien, puede deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2.

Requisitos previos

Asegúrese de que las aplicaciones, los hosts y los servicios que se conecten a Platform Services Controller sean aptos o estén configurados para comunicarse a través de una versión de TLS que permanezca habilitada. Como Platform Services Controller gestiona la autenticación y la administración de certificados, evalúe detenidamente qué servicios pueden verse afectados. Para los servicios que se comunican solamente mediante protocolos no compatibles, la conectividad deja de estar disponible.

Procedimiento

1 Inicie sesión en Platform Services Controller como usuario que puede ejecutar scripts y vaya al directorio donde está ubicado el script.

Sistema operativo	Comando
Windows	`cd %VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator`
Linux	`cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`

2 Puede realizar la tarea en Platform Services Controller en Windows o en el dispositivo de Platform Services Controller.

- Para deshabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	`directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2`
Linux	`directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2`

- Para deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	`directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2`
Linux	`directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2`

3 Si el entorno incluye otros sistemas Platform Services Controller, repita el proceso.

Buscar protocolos TLS habilitados en vCenter Server

Después de habilitar o deshabilitar las versiones de TLS en vCenter Server, puede utilizar la utilidad de configuración de TLS para ver los cambios.

La opción `scan` de la utilidad de configuración de TLS muestra qué versiones de TLS están habilitadas para cada servicio.

Procedimiento

1 Inicie sesión en el sistema vCenter Server.

<table>
<tr><th>Sistema operativo</th><th>Procedimiento</th></tr>
<tr><td>Windows</td><td>a Inicie sesión como usuario con privilegios de administrador.
b Vaya al directorio <code>VcTlsReconfigurator</code>.
<pre>cd %VMWARE_CIS_HOME%
\TlsReconfigurator\VcTlsReconfigurator</pre></td></tr>
<tr><td>Linux</td><td>a Conéctese al dispositivo mediante SSH e inicie sesión como usuario con privilegios para ejecutar scripts.
b Si no está habilitado el shell de Bash, ejecute los siguientes comandos.
<pre>shell.set --enabled true
shell</pre>c Vaya al directorio <code>VcTlsReconfigurator</code>.
<pre>cd /usr/lib/vmware-TlsReconfigurator/
VcTlsReconfigurator</pre></td></tr>
</table>

2 Para mostrar los servicios que tienen TLS habilitado y los puertos utilizados, ejecute el siguiente comando.

```
reconfigureVc scan
```

Revertir los cambios de configuración de TLS

Puede usar la utilidad de configuración de TLS para revertir los cambios de configuración. Al revertir los cambios, el sistema habilita los protocolos que se deshabilitaron mediante la utilidad de configuración de TLS.

Solo se puede llevar a cabo una recuperación si anteriormente se realizó una copia de seguridad de la configuración.

Realice la recuperación en este orden.

1 vSphere Update Manager.

  Si el entorno ejecuta una instancia de vSphere Update Manager distinta en un sistema Windows, primero debe actualizar vSphere Update Manager.

2 vCenter Server.

3 Platform Services Controller.

Requisitos previos

Antes de revertir los cambios, utilice la interfaz de vCenter Server Appliance para realizar una copia de seguridad del dispositivo o equipo Windows.

Procedimiento

1 Conéctese al equipo Windows o al dispositivo.

2 Inicie sesión en el sistema donde desee revertir los cambios.

<table>
<tr><th>Opción</th><th>Descripción</th></tr>
<tr><td>Windows</td><td>a Inicie sesión como usuario con privilegios de administrador.
b Vaya al directorio <code>VcTlsReconfigurator</code>.
<pre>cd %VMWARE_CIS_HOME%
\TlsReconfigurator\VcTlsReconfigurator</pre></td></tr>
<tr><td>Linux</td><td>a Conéctese al dispositivo mediante SSH e inicie sesión como usuario con privilegios para ejecutar scripts.
b Si no está habilitado el shell de Bash, ejecute los siguientes comandos.
<pre>shell.set --enabled true
shell</pre>c Vaya al directorio <code>VcTlsReconfigurator</code>.
<pre>cd /usr/lib/vmware-TlsReconfigurator/
VcTlsReconfigurator</pre></td></tr>
</table>

3 Revise la copia de seguridad anterior.

<table>
<tr><th>Opción</th><th>Descripción</th></tr>
<tr><td>Windows</td><td><pre>C:\ProgramData\VMware\vCenterServer\logs\vmware\vSphere-
TlsReconfigurator\VcTlsReconfigurator.log</pre>El resultado es similar al siguiente ejemplo.
<pre>c:\users\username\appdata\local\temp\20161108T161539
c:\users\username\appdata\local\temp\20161108T171539</pre></td></tr>
<tr><td>Linux</td><td><pre>grep "backup directory" /var/log/vmware/vSphere-
TlsReconfigurator/VcTlsReconfigurator.log</pre>El resultado es similar al siguiente ejemplo.
<pre>2016-11-17T17:29:20.950Z INFO Using backup
directory: /tmp/20161117T172920
2016-11-17T17:32:59.019Z INFO Using backup
directory: /tmp/20161117T173259</pre></td></tr>
</table>

4 Ejecute uno de los siguientes comandos para realizar una restauración.

Opción	Descripción

Windows	`reconfigureVc restore -d Directory_path_from_previous_step`
	Por ejemplo:
	`reconfigureVc restore -d c:\users\username\appdata\local\temp\20161108T171539`

Linux	`reconfigureVc restore -d Directory_path_from_previous_step`
	Por ejemplo:
	`reconfigureVc restore -d /tmp/20161117T172920`

5 Repita el procedimiento en cualquier otra instancia de vCenter Server.

6 Repita el procedimiento en cualquier otra instancia de Platform Services Controller.

Habilitar o deshabilitar las versiones de TLS en vSphere Update Manager en Windows

En vSphere Update Manager 6.7, TLS 1.2 está habilitado de forma predeterminada. TLS 1.0 y TLS 1.1 están deshabilitados de forma predeterminada. Es posible habilitar TLS 1.0 y TLS 1.1, pero no se puede deshabilitar TLS 1.2.

Puede administrar la configuración del protocolo TLS para otros servicios con la utilidad de configuración de TLS. Sin embargo, para vSphere Update Manager en Windows, debe volver a configurar el protocolo TLS manualmente.

La modificación de la configuración del protocolo TLS podría implicar cualquiera de las siguientes tareas.

- Deshabilitar TLS versión 1.0 y dejar habilitados TLS versión 1.1 y TLS 1.2.
- Deshabilitar TLS versión 1.0 y TLS versión 1.1, y dejar habilitado TLS versión 1.2.
- Volver a habilitar una versión de protocolo TLS deshabilitada.

Deshabilitar las versiones anteriores de TLS para Update Manager, puerto 9087

Para deshabilitar las versiones anteriores de TLS para el puerto 9087, modifique el archivo de configuración `jetty-vum-ssl.xml`. El proceso es diferente para el puerto 8084.

Nota Antes de deshabilitar una versión de TLS, asegúrese de que ninguno de los servicios que se comunican con vSphere Update Manager utilice esa versión.

Requisitos previos

Detenga el servicio de vSphere Update Manager. Consulte la documentación de *Instalar y administrar VMware vSphere Update Manager*.

Procedimiento

1 Detenga el servicio de vSphere Update Manager.

2 Desplácese hasta el directorio de instalación de Update Manager, que es diferente para vSphere 6.0, vSphere 6.5 y versiones posteriores.

Versión	Ubicación
vSphere 6.0	`C:\Archivos de programa (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5 y posteriores	`C:\Archivos de programa\VMware\Infrastructure\Update Manager`

3 Realice una copia de seguridad del archivo `jetty-vum-ssl.xml` y abra el archivo.

4 Para deshabilitar las versiones anteriores de TLS, cambie el archivo.

Opción	Descripción

Deshabilite TLS 1.0. Deje TLS 1.1 y TLS 1.2 habilitados.	`<Set name="ExcludeProtocols">`
	`<Array type="java.lang.String">`
	`<Item>TLSv1</Item>`
	`</Array>`
	`</Set>`

Deshabilite TLS 1.0 y TLS 1.1. Deje TLS 1.2 habilitado.	`<Set name="ExcludeProtocols">`
	`<Array type="java.lang.String">`
	`<Item>TLSv1</Item>`
	`<Item>TLSv1.1</Item>`
	`</Array>`
	`</Set>`

5 Guarde el archivo.

6 Reinicie el servicio de vSphere Update Manager.

Deshabilitar las versiones anteriores de TLS para Update Manager, puerto 8084

Para deshabilitar las versiones anteriores de TLS del puerto 8084, modifique el archivo de configuración `vci-integrity.xml`. El proceso es diferente para el puerto 9087.

Nota Antes de deshabilitar una versión de TLS, asegúrese de que ninguno de los servicios que se comunican con vSphere Update Manager utilice esa versión.

Requisitos previos

Detenga el servicio de vSphere Update Manager. Consulte la documentación de *Instalar y administrar VMware vSphere Update Manager*.

Procedimiento

1 Detenga el servicio de vSphere Update Manager.

2 Desplácese hasta el directorio de instalación de Update Manager, que es diferente para 6.0, 6.5 y versiones posteriores.

Versión	Ubicación
vSphere 6.0	`C:\Archivos de programa (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5 y posteriores	`C:\Archivos de programa\VMware\Infrastructure\Update Manager`

3 Realice una copia de seguridad del archivo `vci-integrity.xml` y abra el archivo.

4 Edite el archivo `vci-integrity.xml` y agregue una etiqueta `<protocols>`.

```
<vmacore>
   <ssl>
      <handshakeTimeoutMs>120000</handshakeTimeoutMS>
      <protocols>protocols_value</protocols>
   </ssl>
</vmacore>
```

5 Según la versión de TLS que desee habilitar, utilice uno de los siguientes valores en la etiqueta `<protocols>`.

Versiones de TLS para habilitar	Utilice...
Todo	`tls1.0,tls1.1,tls1.2`.
Solo TLSv1.1 y TLSv.1.2	`tls.1.1,tls1.2`.
Solo TLSv1.2	`tls1.2` o no incluya una etiqueta `protocols`. Debido a que el valor predeterminado es TLS 1.2, no existe ninguna etiqueta `protocols` para empezar en `vmacore`.

6 (opcional) A partir de vSphere 6.0 Update 2, es posible que exista una etiqueta `<sslOptions>`.

Si es así, elimine la etiqueta `<sslOptions>`.

7 Guarde el archivo `vci-integrity.xml`.

8 Reinicie el servicio de vSphere Update Manager.

Volver a habilitar las versiones de TLS deshabilitadas para el puerto 9087 de Update Manager

Si deshabilita una versión de TLS para el puerto 9087 de Update Manager y tiene problemas, puede volver a habilitar la versión. El proceso es diferente para volver a habilitar el puerto 8084.

Volver a habilitar una versión anterior de TLS tiene implicaciones de seguridad.

Procedimiento

1 Detenga el servicio de vSphere Update Manager.

2 Desplácese hasta el directorio de instalación de Update Manager, que es diferente para 6.0, 6.5 y versiones posteriores.

Versión	Ubicación
vSphere 6.0	`C:\Archivos de programa (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5 y posteriores	`C:\Archivos de programa\VMware\Infrastructure\Update Manager`

3 Realice una copia de seguridad del archivo `jetty-vum-ssl.xml` y abra el archivo.

4 Elimine la etiqueta de TLS que corresponde a la versión de protocolo TLS que desea habilitar.

Por ejemplo, elimine `<Item>TLSv1.1</Item>` en el archivo `jetty-vum-ssl.xml` para habilitar TLS v1.1.

5 Guarde el archivo.

6 Reinicie el servicio de vSphere Update Manager.

Volver a habilitar las versiones de TLS deshabilitadas para el puerto 8084 de Update Manager

Si deshabilita una versión de TLS para el puerto 8084 de Update Manager y tiene problemas, puede volver a habilitar la versión. El proceso es diferente para el puerto 9087.

Volver a habilitar una versión anterior de TLS tiene implicaciones de seguridad.

Procedimiento

1 Detenga el servicio de vSphere Update Manager.

2 Desplácese hasta el directorio de instalación de Update Manager, que es diferente para 6.0, 6.5 y versiones posteriores.

Versión	Ubicación
vSphere 6.0	`C:\Archivos de programa (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5 y posteriores	`C:\Archivos de programa\VMware\Infrastructure\Update Manager`

3 Realice una copia de seguridad del archivo `vci-integrity.xml` y abra el archivo.

4 Edite la etiqueta `<protocols>`.

```
 <vmacore>
    <ssl>
       <handshakeTimeoutMs>120000</handshakeTimeoutMS>
       <protocols>protocols_value</protocols>
    </ssl>
</vmacore>
```

5 Según la versión de TLS que desee habilitar, utilice uno de los siguientes valores en la etiqueta `<protocols>`.

Versiones de TLS para habilitar	Utilice...
Todo	`tls1.0,tls1.1,tls1.2`.
Solo TLSv1.1 y TLSv.1.2	`tls.1.1,tls1.2`.
Solo TLSv1.2	`tls1.2` o no incluya una etiqueta `protocols`. Debido a que el valor predeterminado es TLS 1.2, no existe ninguna etiqueta `protocols` para empezar en `vmacore`.

6 Guarde el archivo `vci-integrity.xml`.

7 Reinicie el servicio de vSphere Update Manager.

Privilegios definidos 13

En las siguientes tablas se enumeran los privilegios predeterminados que, cuando se seleccionan para un rol, pueden asignarse a un usuario y a un objeto.

Al establecer permisos, verifique que todos los tipos de objetos estén configurados con los privilegios adecuados para cada acción en particular. Algunas operaciones requieren permiso de acceso en la carpeta raíz o la carpeta primaria además del acceso al objeto que se manipula. Algunas operaciones requieren permiso de acceso o ejecución en la carpeta primaria y un objeto relacionado.

Las extensiones de vCenter Server pueden definir privilegios adicionales que no están indicados aquí. Consulte la documentación relacionada con las extensiones para obtener más información sobre estos privilegios.

Este capítulo incluye los siguientes temas:

- Privilegios de alarmas
- Privilegios de Auto Deploy y perfiles de imagen
- Privilegios de los certificados
- Privilegios de la biblioteca de contenido
- Privilegios de operaciones de cifrado
- Privilegios de centro de datos
- Privilegios de almacenes de datos
- Privilegios de clústeres de almacenes de datos
- Privilegios de Distributed Switch
- Privilegios de ESX Agent Manager
- Privilegios de extensiones
- Privilegios de proveedor de estadísticas externos
- Privilegios de carpeta
- Privilegios globales
- Privilegios de proveedor de actualización de estado

- Privilegios de CIM para hosts
- Privilegios de configuración de hosts
- Inventario del host
- Privilegios de operaciones locales en hosts
- Privilegios de vSphere Replication de host
- Privilegios de perfiles de host
- Privilegios de red
- Privilegios de rendimiento
- Privilegios de permisos
- Privilegios de almacenamiento basado en perfiles
- Privilegios de recursos
- Privilegios para tareas programadas
- Privilegios de sesiones
- Privilegios de vistas de almacenamiento
- Privilegios de tareas
- Privilegios del servicio de transferencia
- Privilegios de configuración de máquinas virtuales
- Privilegios de operaciones de invitado de máquina virtual
- Privilegios para la interacción con máquinas virtuales
- Privilegios de inventario de máquinas virtuales
- Privilegios de aprovisionamiento de las máquinas virtuales
- Privilegios de configuración de servicios de la máquina virtual
- Privilegios de administración de snapshots de las máquinas virtuales
- Privilegios de vSphere Replication de máquinas virtuales
- Privilegios de grupo dvPort
- Privilegios de vApp
- Privilegios de vServices
- Privilegios de etiquetado de vSphere

Privilegios de alarmas

Los privilegios de alarmas controlan la capacidad de crear alarmas, modificarlas y responder a ellas en objetos de inventario.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-1. Privilegios de alarmas

Nombre del privilegio	Descripción	Necesario para
Alarmas.Confirmar alarma	Permite eliminar todas las acciones de todas las alarmas activadas.	Objeto en el que se define una alarma
Alarmas.Crear alarma	Permite crear una alarma nueva. Al crear alarmas con una acción personalizada, se comprueba el privilegio de realizar la acción cuando el usuario crea la alarma.	Objeto en el que se define una alarma
Alarmas.Deshabilitar acción de alarma	Permite evitar que se produzca una acción de alarma después de que se activa la alarma. Esto no deshabilita la alarma.	Objeto en el que se define una alarma
Alarmas.Modificar alarma	Permite cambiar las propiedades de una alarma.	Objeto en el que se define una alarma
Alarmas.Quitar alarma	Permite eliminar una alarma.	Objeto en el que se define una alarma
Alarmas.Establecer estado de alarma	Permite cambiar el estado de la alarma de evento configurada. El estado puede cambiar a **Normal**, **Advertencia** o **Alerta**.	Objeto en el que se define una alarma

Privilegios de Auto Deploy y perfiles de imagen

Los privilegios de Auto Deploy determinan quién puede realizar ciertas tareas en las reglas de Auto Deploy, y quién puede asociar un host. Los privilegios de Auto Deploy también permiten controlar quién puede crear o editar un perfil de imagen.

En la tabla se describen los privilegios que determinan quién puede administrar las reglas y los conjuntos de reglas de Auto Deploy, y quién puede crear y editar perfiles de imagen. Consulte *Instalar y configurar vCenter Server*.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-2. Privilegios de Auto Deploy

Nombre del privilegio	Descripción	Necesario para
Auto Deploy.Host.Equipo asociado	Permite a los usuarios asociar un host a una máquina.	vCenter Server
Auto Deploy.Perfil de imagen.Crear	Permite crear perfiles de imagen.	vCenter Server

Tabla 13-2. Privilegios de Auto Deploy (continuación)

Nombre del privilegio	Descripción	Necesario para
Auto Deploy.Perfil de imagen.Editar	Permite editar perfiles de imagen.	vCenter Server
Auto Deploy.Regla.Crear	Permite crear reglas de Auto Deploy.	vCenter Server
Auto Deploy.Regla.Eliminar	Permite eliminar reglas de Auto Deploy.	vCenter Server
Auto Deploy.Regla.Editar	Permite editar reglas de Auto Deploy.	vCenter Server
Auto Deploy.Conjunto de reglas.Activar	Permite activar conjuntos de reglas de Auto Deploy.	vCenter Server
Auto Deploy.Conjunto de reglas .Editar	Permite editar conjuntos de reglas de Auto Deploy.	vCenter Server

Privilegios de los certificados

Los privilegios de los certificados controlan qué usuarios pueden administrar los certificados de ESXi.

Este privilegio determina quién puede administrar los certificados de los hosts de ESXi. Consulte la sección sobre privilegios necesarios para operaciones de administración de certificados en la documentación de *Administrar Platform Services Controller* para obtener información sobre la administración de certificados de vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-3. Privilegios de los certificados de los hosts

Nombre del privilegio	Descripción	Necesario para
Certificados.Administrar certificados	Permite administrar los certificados de los hosts de ESXi.	vCenter Server

Privilegios de la biblioteca de contenido

Las bibliotecas de contenido ofrecen administración simple y efectiva de plantillas de máquinas virtuales y vApps. Los privilegios de bibliotecas de contenido determinan quién puede ver o administrar diferentes aspectos de las bibliotecas de contenido.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-4. Privilegios de la biblioteca de contenido

Nombre del privilegio	Descripción	Necesario para
Biblioteca de contenido.Agregar elemento de biblioteca	Permite agregar elementos a una biblioteca.	Biblioteca
Biblioteca de contenido.Crear una suscripción a una biblioteca publicada	Permite crear una suscripción a una biblioteca.	Biblioteca
Biblioteca de contenido.Crear biblioteca local	Permite crear bibliotecas locales en el sistema vCenter Server especificado.	vCenter Server
Biblioteca de contenido.Crear biblioteca suscrita	Permite crear bibliotecas suscritas.	vCenter Server
Biblioteca de contenido.Eliminar elemento de biblioteca	Permite eliminar elementos de biblioteca.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.
Biblioteca de contenido.Eliminar biblioteca local	Permite borrar una biblioteca local.	Biblioteca
Biblioteca de contenido.Eliminar biblioteca suscrita	Permite borrar una biblioteca suscrita.	Biblioteca
Biblioteca de contenido.Eliminar una suscripción a una biblioteca publicada	Permite eliminar la suscripción a una biblioteca.	Biblioteca
Biblioteca de contenido.Descargar archivos	Permite descargar archivos de la biblioteca de contenido.	Biblioteca
Biblioteca de contenido.Desalojar elemento de biblioteca	Permite expulsar elementos. El contenido de una biblioteca suscrita puede estar almacenado en caché o no. Si el contenido está almacenado en caché, puede expulsar un elemento de biblioteca para quitarlo (si tiene el privilegio correspondiente).	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.
Biblioteca de contenido.Desalojar biblioteca suscrita	Permite expulsar una biblioteca suscrita. El contenido de una biblioteca suscrita puede estar almacenado en caché o no. Si el contenido está almacenado en caché, puede expulsar una biblioteca para quitarla (si tiene el privilegio correspondiente).	Biblioteca

Tabla 13-4. Privilegios de la biblioteca de contenido (continuación)

Nombre del privilegio	Descripción	Necesario para
Biblioteca de contenido.Importar almacenamiento	Permite a un usuario importar un elemento de biblioteca si la dirección URL del archivo de origen empieza con `ds://` o `file://`. De forma predeterminada, este privilegio está deshabilitado para el administrador de bibliotecas de contenido, ya que una importación desde una dirección URL de almacenamiento implica la importación de contenido. Habilite este privilegio solo si es necesario y si no hay riesgos de seguridad con el usuario que realizará la importación.	Biblioteca
Biblioteca de contenido.Sondear información de suscripción	Este privilegio permite a las API y los usuarios de soluciones sondear la información de suscripción de una biblioteca remota, como su dirección URL, certificado SSL y contraseña. La estructura que se obtiene describe si la configuración de suscripción es correcta o si hay problemas, como errores de SSL.	Biblioteca
Biblioteca de contenido.Publicar un elemento de la biblioteca para los suscriptores	Permite publicar elementos de biblioteca para suscriptores.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.
Biblioteca de contenido.Publicar una biblioteca para los suscriptores	Permite publicar las bibliotecas para suscriptores.	Biblioteca
Biblioteca de contenido.Leer almacenamiento	Permite leer el almacenamiento de una biblioteca de contenido.	Biblioteca
Biblioteca de contenido.Sincronizar elemento de biblioteca	Permite sincronizar elementos de biblioteca.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.
Biblioteca de contenido.Sincronizar biblioteca suscrita	Permite sincronizar bibliotecas suscritas.	Biblioteca
Biblioteca de contenido.Escribir introspección	Permite a un usuario de solución o a una API revisar los complementos de compatibilidad de tipos del servicio de biblioteca de contenido.	Biblioteca
Biblioteca de contenido.Actualizar parámetros de configuración	Permite actualizar los valores de configuración. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	Biblioteca
Biblioteca de contenido.Actualizar archivos	Permite cargar contenido a la biblioteca de contenido. También permite eliminar archivos de un elemento de biblioteca.	Biblioteca
Biblioteca de contenido.Actualizar biblioteca	Permite actualizar la biblioteca de contenido.	Biblioteca

Tabla 13-4. Privilegios de la biblioteca de contenido (continuación)

Nombre del privilegio	Descripción	Necesario para
Biblioteca de contenido.Actualizar elemento de biblioteca	Permite actualizar elementos de biblioteca.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.
Biblioteca de contenido.Actualizar biblioteca local	Permite actualizar bibliotecas locales.	Biblioteca
Biblioteca de contenido.Actualizar biblioteca suscrita	Permite actualizar las propiedades de una biblioteca suscrita.	Biblioteca
Biblioteca de contenido.Actualizar una suscripción a una biblioteca publicada	Permite realizar actualizaciones en los parámetros de suscripción. Los usuarios pueden actualizar parámetros como la especificación de la instancia de vCenter Server de la biblioteca suscrita y la colocación de sus elementos de plantilla de máquina virtual.	Biblioteca
Biblioteca de contenido.Ver parámetros de configuración	Permite ver las opciones de configuración. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	Biblioteca

Privilegios de operaciones de cifrado

Los privilegios de operaciones de cifrado controlan quién puede realizar qué tipo de operación de cifrado en qué tipo de objeto.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-5. Privilegios de operaciones de cifrado

Nombre del privilegio	Descripción	Necesario para
Operaciones de cifrado.Acceso directo	Permite que los usuarios accedan a los recursos cifrados. Por ejemplo, los usuarios pueden exportar máquinas virtuales, tener acceso NFC a las máquinas virtuales, etc.	Máquina virtual, host o almacén de datos
Operaciones de cifrado.Agregar disco	Permite que los usuarios agreguen un disco a una máquina virtual cifrada.	Máquina virtual
Operaciones de cifrado.Clonar	Permite que los usuarios clonen una máquina virtual cifrada.	Máquina virtual

Tabla 13-5. Privilegios de operaciones de cifrado (continuación)

Nombre del privilegio	Descripción	Necesario para
Operaciones de cifrado.Descifrar	Permite que los usuarios descifren una máquina virtual o un disco.	Máquina virtual
Operaciones de cifrado.Cifrar	Permite que los usuarios cifren una máquina virtual o un disco de máquina virtual.	Máquina virtual
Operaciones de cifrado.Cifrar nuevo	Permite que los usuarios cifren una máquina virtual durante la creación de una máquina virtual o un disco durante la creación de un disco.	Carpeta de máquina virtual
Operaciones de cifrado.Administrar directivas de cifrado	Permite que los usuarios administren las directivas de almacenamiento de la máquina virtual con filtros de E/S de cifrado. De forma predeterminada, las máquinas virtuales que utilizan la directiva de almacenamiento Cifrado no utilizan otras directivas de almacenamiento.	Carpeta raíz de vCenter Server
Operaciones de cifrado.Administrar servidores de claves	Permite que los usuarios administren el servidor de administración de claves (Key Management Server, KMS) para el sistema vCenter Server. Entre las tareas de administración, se incluyen agregar y eliminar instancias de KMS y establecer una relación de confianza con el KMS.	Sistema vCenter Server
Operaciones de cifrado.Administrar claves	Permite que los usuarios realicen operaciones de administración de claves. Estas operaciones no se admiten en vSphere Web Client, pero se pueden realizar mediante el uso de `crypto-util` o la API.	Carpeta raíz de vCenter Server
Operaciones de cifrado.Migrar	Permite que los usuarios migren una máquina virtual cifrada a un host ESXi distinto. Admite la migración con o sin vMotion y Storage vMotion. No admite la migración a una instancia de vCenter Server distinta.	Máquina virtual

Tabla 13-5. Privilegios de operaciones de cifrado (continuación)

Nombre del privilegio	Descripción	Necesario para
Operaciones de cifrado.Volver a cifrar	Permite que los usuarios vuelvan a cifrar máquinas virtuales o discos con una clave distinta. Este privilegio es necesario para las operaciones de repetición de cifrado profundo y superficial.	Máquina virtual
Operaciones de cifrado.Registrar máquina virtual	Permite que los usuarios registren una máquina virtual cifrada con un host ESXi.	Carpeta de máquina virtual
Operaciones de cifrado.Registrar host	Permite que los usuarios habiliten el cifrado en un host. El cifrado en un host se puede habilitar de forma explícita o mediante el proceso de creación de máquinas virtuales.	Carpeta de hosts para los hosts independientes, clúster para los hosts del clúster

Privilegios de centro de datos

Los privilegios de centro de datos controlan la habilidad para crear y editar centros de datos en el inventario vSphere Web Client.

Todos los privilegios de centros de datos se utilizan solamente en vCenter Server. El privilegio **Crear centro de datos** se define en carpetas del centro de datos o el objeto raíz. Todos los demás privilegios de centros de datos se emparejan con centros de datos, carpetas de centros de datos o el objeto raíz.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-6. Privilegios de centro de datos

Nombre del privilegio	Descripción	Necesario para
Centro de datos.Crear centro de datos	Permite la creación de un nuevo centro de datos.	Carpeta de centro de datos u objeto raíz
Centro de datos.Mover centro de datos	Permite mover un centro de datos. El privilegio debe estar presente tanto en el origen como en el destino.	Centro de datos, origen y destino
Centro de datos.Configuración de perfil de protocolo de red	Permite la configuración del perfil de red para un centro de datos.	Centro de datos
Centro de datos.Consultar asignación de grupo de direcciones IP	Permite la configuración de un grupo de direcciones IP.	Centro de datos
Centro de datos.Volver a configurar centro de datos	Permite la reconfiguración de un centro de datos.	Centro de datos

Tabla 13-6. Privilegios de centro de datos (continuación)

Nombre del privilegio	Descripción	Necesario para
Centro de datos.Liberar asignación de IP	Permite liberar la asignación de IP asignada para un centro de datos.	Centro de datos
Centro de datos.Quitar centro de datos	Permite la eliminación de un centro de datos. Para tener los permisos necesarios para realizar esta operación, debe tener este privilegio asignado tanto en el objeto como en su objeto primario.	Centro de datos más objeto primario
Centro de datos.Cambiar nombre de centro de datos	Permite cambiarle el nombre a un centro de datos.	Centro de datos

Privilegios de almacenes de datos

Los privilegios de almacenes de datos controlan la capacidad para examinar y administrar almacenes de datos, así como para asignar espacios en ellos.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-7. Privilegios de almacenes de datos

Nombre del privilegio	Descripción	Necesario para
Almacén de datos.Asignar espacio	Permite asignar un espacio en un almacén de datos de una máquina virtual, una instantánea, un clon o un disco virtual.	Almacenes de datos
Almacén de datos.Examinar almacén de datos	Permite desplazarse hasta archivos de un almacén de datos.	Almacenes de datos
Almacén de datos.Configurar almacén de datos	Permite configurar un almacén de datos.	Almacenes de datos
Almacén de datos.Operaciones de archivos de bajo nivel	Permite realizar tareas de lectura, escritura, eliminación y cambio de nombre en el explorador del almacén de datos.	Almacenes de datos
Almacén de datos.Mover almacén de datos	Permite mover un almacén de datos entre diferentes carpetas. Los privilegios deben estar presentes tanto en el origen como en el destino.	Almacén de datos, origen y destino
Almacén de datos.Quitar almacén de datos	Permite quitar un almacén de datos. Este privilegio es obsoleto. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Almacenes de datos
Almacén de datos.Quitar archivo	Permite eliminar archivos del almacén de datos. Este privilegio es obsoleto. Asigne el privilegio **Operaciones de archivos de nivel bajo**.	Almacenes de datos

Tabla 13-7. Privilegios de almacenes de datos (continuación)

Nombre del privilegio	Descripción	Necesario para
Almacén de datos.Cambiar nombre de almacén de datos	Permite cambiar el nombre de un almacén de datos.	Almacenes de datos
Almacén de datos.Actualizar archivos de la máquina virtual	Permite actualizar las rutas de acceso de los archivos de máquinas virtuales en un almacén de datos una vez que el almacén de datos se volvió a firmar.	Almacenes de datos
Almacén de datos.Actualizar metadatos de la máquina virtual	Permite actualizar los metadatos de máquina virtual asociados con un almacén de datos.	Almacenes de datos

Privilegios de clústeres de almacenes de datos

Los privilegios de clústeres de almacenes de datos controlan la configuración de clústeres de almacenes de datos de Storage DRS.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-8. Privilegios de clústeres de almacenes de datos

Nombre del privilegio	Descripción	Necesario para
Clúster de almacenes de datos.Configurar un clúster de almacenes de datos	Permite crear y configurar parámetros para los clústeres de almacenes de datos de Storage DRS.	Clústeres de almacenes de datos

Privilegios de Distributed Switch

Los privilegios de Distributed Switch controlan la capacidad para realizar tareas relacionadas con la administración de las instancias de Distributed Switch.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-9. Privilegios de vSphere Distributed Switch

Nombre del privilegio	Descripción	Necesario para
Distributed Switch.Crear	Permite crear un conmutador distribuido.	Centros de datos, carpetas de red
Distributed Switch.Eliminar	Permite quitar un conmutador distribuido. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Conmutadores distribuidos
Distributed Switch.Operación de host	Permite cambiar los miembros de host de un conmutador distribuido.	Conmutadores distribuidos
Distributed Switch.Modificar	Permite cambiar la configuración de un conmutador distribuido.	Conmutadores distribuidos
Distributed Switch.Mover	Permite mover vSphere Distributed Switch a otra carpeta.	Conmutadores distribuidos
Distributed Switch.Operación Network I/O Control	Permite cambiar la configuración de los recursos de vSphere Distributed Switch.	Conmutadores distribuidos
Distributed Switch.Operación de directiva	Permite cambiar la directiva de vSphere Distributed Switch.	Conmutadores distribuidos
Distributed Switch .Operación de configuración de puerto	Permite cambiar los parámetros de un puerto en vSphere Distributed Switch.	Conmutadores distribuidos
Distributed Switch.Operación de configuración de puerto	Permite cambiar la configuración de un puerto en vSphere Distributed Switch.	Conmutadores distribuidos
Distributed Switch.Operación de VSPAN	Permite cambiar la configuración de VSPAN de vSphere Distributed Switch.	Conmutadores distribuidos

Privilegios de ESX Agent Manager

Los privilegios de ESX Agent Manager controlan las operaciones relacionadas con ESX Agent Manager y las máquinas virtuales de agentes. ESX Agent Manager es un servicio que permite instalar máquinas virtuales de administración asociadas a un host que no se ven afectadas por VMware DRS u otros servicios de migración de máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-10. ESX Agent Manager

Nombre del privilegio	Descripción	Necesario para
ESX Agent Manager.Configurar	Permite implementar la máquina virtual de un agente en un host o un clúster.	Máquinas virtuales
ESX Agent Manager.Modificar	Permite modificar la máquina virtual de un agente, por ejemplo, apagar o eliminar la máquina virtual.	Máquinas virtuales
Vista de ESX Agent.Ver	Permite ver la máquina virtual de un agente.	Máquinas virtuales

Privilegios de extensiones

Los privilegios de extensiones controlan la capacidad para instalar y administrar extensiones.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-11. Privilegios de extensiones

Nombre del privilegio	Descripción	Necesario para
Extensión.Registrar extensión	Permite registrar una extensión (complemento).	vCenter Server raíz
Extensión.Eliminar extensión del registro	Permite anular el registro de una extensión (complemento).	vCenter Server raíz
Extensión.Actualizar extensión	Permite actualizar una extensión (complemento).	vCenter Server raíz

Privilegios de proveedor de estadísticas externos

Los privilegios del proveedor de estadísticas externo controlan la capacidad para notificar a vCenter Server sobre las estadísticas de Distributed Resource Scheduler (DRS) proactivo.

Estos privilegios solo se aplican a las API internas de VMware.

Privilegios de carpeta

Estos privilegios controlan la capacidad para crear y administrar carpetas.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-12. Privilegios de carpeta

Nombre del privilegio	Descripción	Necesario para
Carpeta.Crear carpeta	Permite crear una carpeta nueva.	Carpetas
Carpeta.Eliminar carpeta	Permite eliminar una carpeta. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Carpetas
Carpeta.Mover carpeta	Permite mover una carpeta. El privilegio debe estar presente tanto en el origen como en el destino.	Carpetas
Carpeta.Cambiar nombre de carpeta	Permite cambiarle el nombre a una carpeta.	Carpetas

Privilegios globales

Los privilegios globales controlan tareas globales relacionadas con tareas, scripts y extensiones.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-13. Privilegios globales

Nombre del privilegio	Descripción	Necesario para
Global.Actuar como vCenter Server	Permite preparar e iniciar una operación de envío o recepción de vMotion.	vCenter Server raíz
Global.Cancelar tarea	Permite cancelar una tarea en cola o en ejecución.	Objeto de inventario relacionado con la tarea
Global.Planificación de capacidad	Permite habilitar el uso de la planificación de capacidad para la consolidación de planificación de máquinas físicas en máquinas virtuales.	vCenter Server raíz
Global.Diagnósticos	Permite recuperar una lista de archivos de diagnóstico, encabezados de registro, archivos binarios o paquetes de diagnóstico. Para evitar infracciones de seguridad potenciales, limite este privilegio a la función de administrador de vCenter Server.	vCenter Server raíz
Global.Deshabilitar métodos	Permite a los servidores de las extensiones de vCenter Server deshabilitar ciertas operaciones en objetos administrados con vCenter Server.	vCenter Server raíz
Global.Habilitar métodos	Permite a los servidores de las extensiones de vCenter Server habilitar ciertas operaciones en objetos administrados con vCenter Server.	vCenter Server raíz
Global.Etiqueta global	Permite agregar o quitar etiquetas globales.	Host raíz o vCenter Server

Tabla 13-13. Privilegios globales (continuación)

Nombre del privilegio	Descripción	Necesario para
Global.Estado	Permite ver el estado de los componentes de vCenter Server.	vCenter Server raíz
Global.Licencias	Permite ver las licencias instaladas y agregar o quitar licencias.	Host raíz o vCenter Server
Global.Registrar evento	Permite registrar un evento definido por el usuario ante una entidad administrada en particular.	Cualquier objeto
Global.Administrar atributos personalizados	Permite agregar y quitar definiciones de campo personalizadas, así como cambiar sus nombres.	vCenter Server raíz
Global.Proxy	Permite acceder a una interfaz interna para agregar o quitar puntos extremos en el proxy o desde él.	vCenter Server raíz
Global.Acción de script	Permite programar una acción generada por script junto con una alarma.	Cualquier objeto
Global.Administradores de servicios	Permite utilizar el comando `resxtop` en vSphere CLI.	Host raíz o vCenter Server
Global.Configurar atributo personalizado	Permite ver, crear o quitar atributos personalizados para un objeto administrado.	Cualquier objeto
Global.Configuración	Permite leer y modificar las opciones de configuración de vCenter Server de tiempo de ejecución.	vCenter Server raíz
Global.Etiqueta del sistema	Permite agregar o quitar etiquetas de sistema.	vCenter Server raíz

Privilegios de proveedor de actualización de estado

Los privilegios del proveedor de actualizaciones de estado controlan la capacidad de los proveedores de hardware para notificar a vCenter Server sobre los eventos proactivos de HA.

Estos privilegios solo se aplican a las API internas de VMware.

Privilegios de CIM para hosts

Los privilegios de CIM para hosts controlan el uso de CIM para supervisar el estado de los hosts.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-14. Privilegios de CIM para hosts

Nombre del privilegio	Descripción	Necesario para
Host.CIM.Interacción de CIM	Permite que un cliente obtenga un vale para usar los servicios de CIM.	Hosts

Privilegios de configuración de hosts

Los privilegios de configuración de hosts controlan la capacidad para configurar hosts.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-15. Privilegios de configuración de hosts

Nombre del privilegio	Descripción	Necesario para
Host.Configuración.Configuración avanzada	Permite establecer las opciones de configuración avanzada del host.	Hosts
Host.Configuración.Almacén de autenticación	Permite configurar los almacenes de autenticación de Active Directory.	Hosts
Host.Configuración.Cambiar configuración de PciPassthru	Permite cambiar la configuración de PciPassthru de un host.	Hosts
Host.Configuración.Cambiar configuración de SNMP	Permite cambiar la configuración de SNMP de un host.	Hosts
Host.Configuración.Cambiar configuración de fecha y hora	Permite cambiar la configuración de fecha y hora de un host.	Hosts
Host.Configuración.Cambiar configuración	Permite configurar el modo de bloqueo de los hosts ESXi.	Hosts
Host.Configuración.Conexión	Permite cambiar el estado de conexión de un host (conectado o desconectado).	Hosts
Host.Configuración.Firmware	Permite actualizar el firmware del host ESXi.	Hosts
Host.Configuración.Hiperproceso	Permite habilitar y deshabilitar la función de hiperproceso en el programador de la CPU del host.	Hosts
Host.Configuración.Configuración de imagen	Permite cambiar la imagen asociada a un host.	
Host.Configuración.Mantenimiento	Permite que el host entre y salga del modo de mantenimiento, y apagar y reiniciar el host.	Hosts
Host.Configuración.Configuración de memoria	Permite modificar la configuración del host.	Hosts
Host.Configuración.Configuración de red	Permite configurar la red, el firewall y la red vMotion.	Hosts
Host.Configuración.Alimentación	Permite configurar las opciones de administración de energía del host.	Hosts
Host.Configuración.Consultar revisión	Permite consultar las revisiones instalables e instalar revisiones en el host.	Hosts
Host.Configuración.Perfil de seguridad y firewall	Permite configurar los servicios de Internet, como SSH, Telnet, SNMP y del firewall del host.	Hosts

Tabla 13-15. Privilegios de configuración de hosts (continuación)

Nombre del privilegio	Descripción	Necesario para
Host.Configuración.Configuración de partición de almacenamiento	Permite administrar la partición de diagnóstico y el almacén de datos de VMFS. Los usuarios con este privilegio pueden examinar dispositivos de almacenamiento nuevos y administrar iSCSI.	Hosts
Host.Configuración.Administración del sistema	Permite que las extensiones manipulen el sistema de archivos del host.	Hosts
Host.Configuración.Recursos del sistema	Permite actualizar la configuración de la jerarquía de recursos del sistema.	Hosts
Host.Configuración.Configuración de inicio automático de la máquina virtual	Permite cambiar el orden de inicio e interrupción automáticos de las máquinas virtuales de un solo host.	Hosts

Inventario del host

Los privilegios de inventario de host controlan las operaciones de agregar hosts al inventario y a los clústeres, y de mover los hosts en el inventario.

En la tabla se describen los privilegios necesarios para agregar y mover hosts y clústeres en el inventario.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-16. Privilegios de inventario de host

Nombre del privilegio	Descripción	Necesario para
Host.Inventario.Agregar host a clúster	Permite agregar un host a un clúster que ya existe.	Clústeres
Host.Inventario.Agregar host independiente	Permite agregar un host independiente.	Carpetas de hosts
Host.Inventario.Crear clúster	Permite crear un nuevo clúster.	Carpetas de hosts
Host.Inventario.Modificar clúster	Permite cambiar las propiedades de un clúster.	Clústeres
Host.Inventario.Mover clúster o host independiente	Permite mover un clúster o un host independiente entre carpetas. El privilegio debe estar presente tanto en el origen como en el destino.	Clústeres
Host.Inventario.Mover host	Permite mover un conjunto de hosts existentes hacia adentro o afuera de un clúster. El privilegio debe estar presente tanto en el origen como en el destino.	Clústeres

Tabla 13-16. Privilegios de inventario de host (continuación)

Nombre del privilegio	Descripción	Necesario para
Host.Inventario.Quitar clúster	Permite eliminar un clúster o un host independiente. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Clústeres, hosts
Host.Inventario.Quitar host	Permite quitar un host. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Hosts más objeto primario
Host.Inventario.Cambiar nombre de clúster	Permite cambiar el nombre de un clúster.	Clústeres

Privilegios de operaciones locales en hosts

Los privilegios de operaciones locales en hosts controlan las acciones que se realizan cuando VMware Host Client está conectado directamente a un host.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-17. Privilegios de operaciones locales en hosts

Nombre del privilegio	Descripción	Necesario para
Host.Operaciones locales.Agregar host a vCenter	Permite instalar y quitar agentes de vCenter, como vpxa y aam, en un host.	Host raíz
Host.Operaciones locales.Crear máquina virtual	Permite crear una máquina virtual nueva desde cero en un disco sin registrarla en el host.	Host raíz
Host.Operaciones locales.Eliminar máquina virtual	Permite eliminar una máquina virtual del disco. Esta operación se admite para máquinas virtuales registradas o no registradas.	Host raíz
Host.Operaciones locales.Administrar grupos de usuarios	Permite administrar cuentas locales en un host.	Host raíz
Host.Operaciones locales.Volver a configurar máquina virtual	Permite volver a configurar una máquina virtual.	Host raíz

Privilegios de vSphere Replication de host

Los privilegios de vSphere Replication de host controlan la utilización de la replicación de máquinas virtuales que realiza VMware vCenter Site Recovery Manager™ para un host.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-18. Privilegios de vSphere Replication de host

Nombre del privilegio	Descripción	Necesario para
Host.vSphere Replication.Administrar replicación	Permite administrar la replicación de máquinas virtuales en este host.	Hosts

Privilegios de perfiles de host

Los privilegios de perfiles de host controlan las operaciones relacionadas con la creación y la modificación de perfiles de host.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-19. Privilegios de perfiles de host

Nombre del privilegio	Descripción	Necesario para
Perfil de host.Borrar	Permite borrar información relacionada con el perfil.	vCenter Server raíz
Perfil de host.Crear	Permite crear un perfil de host.	vCenter Server raíz
Perfil de host.Eliminar	Permite eliminar un perfil de host.	vCenter Server raíz
Perfil de host.Editar	Permite editar un perfil de host.	vCenter Server raíz
Perfil de host.Exportar	Permite exportar un perfil de host.	vCenter Server raíz
Perfil de host.Ver	Permite ver un perfil de host.	vCenter Server raíz

Privilegios de red

Los privilegios de red controlan las tareas relacionadas con la administración de redes.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-20. Privilegios de red

Nombre del privilegio	Descripción	Necesario para
Red.Asignar red	Permite asignar una red a una máquina virtual.	Redes, máquinas virtuales
Red.Configurar	Permite configurar una red.	Redes, máquinas virtuales
Red.Mover red	Permite mover una red entre carpetas. El privilegio debe estar presente tanto en el origen como en el destino.	Redes
Red.Quitar	Permite eliminar una red. Este privilegio es obsoleto. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Redes

Privilegios de rendimiento

Los privilegios de rendimiento controlan la modificación de la configuración de estadísticas de rendimiento.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-21. Privilegios de rendimiento

Nombre del privilegio	Descripción	Necesario para
Rendimiento.Modificar intervalos	Permite crear, quitar y actualizar intervalos de recopilación de datos de rendimiento.	vCenter Server raíz

Privilegios de permisos

Los privilegios de permisos controlan la asignación de funciones y permisos.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-22. Privilegios de permisos

Nombre del privilegio	Descripción	Necesario para
Permisos.Modificar permiso	Permite definir una o más reglas de permiso en una entidad, o actualizar reglas si estas ya están presentes para un usuario o grupo determinados en la entidad. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Cualquier objeto más objeto primario
Permisos.Modificar privilegio	Permite modificar un grupo o una descripción del privilegio. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	
Permisos.Modificar función	Permite actualizar el nombre de una función y los privilegios asociados con esa función.	Cualquier objeto
Permisos.Reasignar permisos de función	Permite reasignar todos los permisos de una función a otra.	Cualquier objeto

Privilegios de almacenamiento basado en perfiles

Los privilegios de almacenamiento basado en perfiles controlan las operaciones relacionadas con los perfiles de almacenamiento.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-23. Privilegios de almacenamiento basado en perfiles

Nombre del privilegio	Descripción	Necesario para
Almacenamiento basado en perfiles.Actualización de almacenamiento basado en perfiles	Permite realizar cambios en los perfiles de almacenamiento, por ejemplo, crear y actualizar capacidades de almacenamiento y perfiles de almacenamiento de máquinas virtuales.	vCenter Server raíz
Almacenamiento basado en perfiles.Vista de almacenamiento basado en perfiles	Permite ver las capacidades de almacenamiento y los perfiles de almacenamiento definidos.	vCenter Server raíz

Privilegios de recursos

Los privilegios de recursos controlan la creación y la administración de grupos de recursos, como también la migración de máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-24. Privilegios de recursos

Nombre del privilegio	Descripción	Necesario para
Recurso.Aplicar recomendación	Permite aceptar una sugerencia del servidor para realizar una migración con vMotion.	Clústeres
Recurso.Asignar vApp a grupo de recursos	Permite asignar una vApp a un grupo de recursos.	Grupos de recursos
Recurso.Asignar máquina virtual a grupo de recursos	Permite asignar una máquina virtual a un grupo de recursos.	Grupos de recursos
Recurso.Crear grupo de recursos	Permite crear grupos de recursos.	Grupos de recursos, clústeres
Recurso.Migrar máquina virtual apagada	Permite migrar una máquina virtual apagada a un grupo de recursos o host diferentes.	Máquinas virtuales
Recurso.Migrar máquina virtual encendida	Permite migrar con vMotion una máquina virtual encendida a un grupo de recursos o host diferentes.	
Recurso.Modificar grupo de recursos	Permite cambiar las asignaciones de un grupo de recursos.	Grupos de recursos
Recurso.Mover grupo de recursos	Permite mover un grupo de recursos. El privilegio debe estar presente tanto en el origen como en el destino.	Grupos de recursos
Recurso.Consultar vMotion	Permite consultar la compatibilidad general de vMotion de una máquina virtual con un conjunto de hosts.	vCenter Server raíz
Recurso.Quitar grupo de recursos	Permite eliminar un grupo de recursos. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Grupos de recursos
Recurso.Cambiar nombre de grupo de recursos	Permite cambiar el nombre a un grupo de recursos.	Grupos de recursos

Privilegios para tareas programadas

Estos privilegios controlan la creación, la edición y la eliminación de tareas programadas.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-25. Privilegios para tareas programadas

Nombre del privilegio	Descripción	Necesario para
Tarea programada.Crear tareas	Permite programar una tarea. Se lo requiere, junto con los privilegios, para realizar la acción programada en el momento de la programación.	Cualquier objeto
Tarea programada.Modificar tarea	Permite volver a configurar las propiedades de la tarea programada.	Cualquier objeto
Tarea programada.Quitar tarea	Permite quitar una tarea programada de la cola.	Cualquier objeto
Tarea programada.Ejecutar tarea	Permite ejecutar la tarea programada de inmediato. Para crear y ejecutar una tarea programada también se necesitan permisos para la acción asociada.	Cualquier objeto

Privilegios de sesiones

Los privilegios de sesiones controlan la capacidad de las extensiones para abrir sesiones en el sistema vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-26. Privilegios de sesiones

Nombre del privilegio	Descripción	Necesario para
Sesiones.Suplantar usuario	Permiten suplantar a otro usuario. Esta capacidad se utiliza con las extensiones.	vCenter Server raíz
Sesiones.Mensaje	Permiten configurar el mensaje de inicio sesión global.	vCenter Server raíz
Sesiones.Validar sesión	Permiten verificar la validez de la sesión.	vCenter Server raíz
Sesiones.Ver y detener sesiones	Permiten visualizar sesiones y forzar el cierre de sesión de uno o más usuarios conectados.	vCenter Server raíz

Privilegios de vistas de almacenamiento

Los privilegios de vistas de almacenamiento controlan los privilegios de las API de servicio de supervisión de almacenamiento.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-27. Privilegios de vistas de almacenamiento

Nombre del privilegio	Descripción	Necesario para
Vistas de almacenamiento.Configurar servicio	Permite a los usuarios con privilegios utilizar todas las API del servicio de supervisión de almacenamiento. Utilice **Vistas de almacenamiento.Ver** para los privilegios sobre las API de solo lectura del servicio de supervisión de almacenamiento.	vCenter Server raíz
Vistas de almacenamiento.Ver	Permite a los usuarios con privilegios utilizar las API de solo lectura del servicio de supervisión de almacenamiento.	vCenter Server raíz

Privilegios de tareas

Los privilegios de tareas controlan la capacidad de las extensiones de crear y actualizar tareas en vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-28. Privilegios de tareas

Nombre del privilegio	Descripción	Necesario para
Tareas.Crear tarea	Permite que una extensión cree una tarea definida por el usuario. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	vCenter Server raíz
Tareas.Actualizar tarea	Permite que una extensión actualice una tarea definida por el usuario. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	vCenter Server raíz

Privilegios del servicio de transferencia

Los privilegios de servicio de transferencia son internos de VMware. No utilice estos privilegios.

Privilegios de configuración de máquinas virtuales

Los privilegios de configuración de máquinas virtuales controlan la capacidad de configurar opciones y dispositivos de máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-29. Privilegios de configuración de máquinas virtuales

Nombre del privilegio	Descripción	Necesario para
Máquina virtual.Configuración.Adquirir concesión de discos	Permite realizar operaciones de concesión de discos para una máquina virtual.	Máquinas virtuales
Máquina virtual.Configuración.Agregar un disco existente	Permite agregar un disco virtual existente a una máquina virtual.	Máquinas virtuales
Máquina virtual.Configuración.Agregar disco nuevo	Permite crear un disco virtual nuevo para agregar a una máquina virtual.	Máquinas virtuales
Máquina virtual.Configuración.Agregar o quitar dispositivo	Permite agregar o eliminar cualquier dispositivo que no sea un disco.	Máquinas virtuales
Máquina virtual.Configuración.Configuración avanzada	Permite agregar o modificar parámetros avanzados en el archivo de configuración de la máquina virtual.	Máquinas virtuales
Máquina virtual.Configuración.Cambiar recuento de CPU	Permite cambiar la cantidad de CPU virtuales.	Máquinas virtuales
Máquina virtual.Configuración.Cambiar memoria	Permite cambiar la cantidad de memoria asignada a la máquina virtual.	Máquinas virtuales
Máquina virtual.Configuración.Cambiar ajustes	Permite cambiar la configuración general de la máquina virtual.	Máquinas virtuales
Máquina virtual.Configuración.Cambiar ubicación de archivo de intercambio	Permite cambiar la directiva de selección del archivo de intercambio de una máquina virtual.	Máquinas virtuales
Máquina virtual.Configuración.Cambiar recurso	Permite cambiar la configuración de recursos de un conjunto de nodos de máquinas virtuales en un grupo de recursos determinado.	Máquinas virtuales
Máquina virtual.Configuración.Configurar dispositivo USB de host	Permite conectar un dispositivo USB basado en host a una máquina virtual.	Máquinas virtuales

Tabla 13-29. Privilegios de configuración de máquinas virtuales (continuación)

Nombre del privilegio	Descripción	Necesario para
Máquina virtual.Configuración.Configurar dispositivo sin formato	Permite agregar y eliminar una asignación de discos sin formato o un dispositivo de acceso directo de SCSI. Al configurar este parámetro, se anula cualquier otro privilegio de modificación de dispositivos sin procesar, incluidos los estados de conexión.	Máquinas virtuales
Máquina virtual.Configuración.Configurar managedBy	Permite que una extensión o solución marque una máquina virtual como administrada por ella.	Máquinas virtuales
Máquina virtual.Configuración.Mostrar configuración de conexión	Permite configurar opciones de consola remota de máquinas virtuales.	Máquinas virtuales
Máquina virtual.Configuración.Extender disco virtual	Permite expandir el tamaño de un disco virtual.	Máquinas virtuales
Máquina virtual.Configuración.Modificar configuración de dispositivos	Permite cambiar las propiedades de un dispositivo existente.	Máquinas virtuales
Máquina virtual.Configuración.Consultar compatibilidad con Fault Tolerance	Permite comprobar si una máquina virtual es compatible con Fault Tolerance.	Máquinas virtuales
Máquina virtual.Configuración.Consulta archivos sin propietario	Permite consultar archivos sin propietario.	Máquinas virtuales
Máquina virtual.Configuración.Volver a cargar desde la ruta de acceso	Permite cambiar la ruta de acceso de configuración de una máquina virtual y, a la vez, preservar la identidad de esta última. Las soluciones como vCenter Site Recovery Manager de VMware usan esta operación para resguardar la identidad de la máquina virtual durante la conmutación por error y la conmutación por recuperación.	Máquinas virtuales
Máquina virtual.Configuración.Quitar disco	Permite extraer el dispositivo de disco virtual.	Máquinas virtuales
Máquina virtual.Configuración.Cambiar nombre	Permite cambiar el nombre de una máquina virtual o modificar las notas asociadas de una máquina virtual.	Máquinas virtuales
Máquina virtual.Configuración.Restablecer información del invitado	Permite editar la información de sistemas operativos invitados de una máquina virtual.	Máquinas virtuales

Tabla 13-29. Privilegios de configuración de máquinas virtuales (continuación)

Nombre del privilegio	Descripción	Necesario para
Máquina virtual.Configuración.Configurar anotación	Permite agregar o editar una anotación de máquina virtual.	Máquinas virtuales
Máquina virtual.Configuración.Alternar seguimiento de cambios de disco	Permite habilitar o deshabilitar el seguimiento de cambios para los discos de la máquina virtual.	Máquinas virtuales
Máquina virtual.Configuración.Alternar objeto primario de bifurcación	Permite habilitar o deshabilitar un elemento principal de vmfork.	Máquinas virtuales
Máquina virtual.Configuración.Actualizar compatibilidad de la máquina virtual	Permite actualizar la versión de compatibilidad de la máquina virtual.	Máquinas virtuales

Privilegios de operaciones de invitado de máquina virtual

Los privilegios de operaciones de invitado de máquina virtual controlan la capacidad de interacción con los archivos y los programas que se encuentran en el sistema operativo invitado de una máquina virtual con la API.

Consulte la documentación sobre la *referencia de VMware vSphere API* para obtener más información sobre dichas operaciones.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-30. Operaciones de invitado de la máquina virtual

Nombre del privilegio	Descripción	Efectivo en el objeto
Máquina virtual.Operaciones de invitado.Modificación de alias de operaciones de invitado	Permite las operaciones de invitado de máquina virtual que implican modificar el alias de la máquina virtual.	Máquinas virtuales
Máquina virtual.Operaciones de invitado.Consulta de alias de operaciones de invitado	Permite las operaciones de invitado de máquina virtual que implican consultar el alias de la máquina virtual.	Máquinas virtuales

Tabla 13-30. Operaciones de invitado de la máquina virtual (continuación)

Nombre del privilegio	Descripción	Efectivo en el objeto
Máquina virtual.Operaciones de invitado.Modificaciones de operaciones de invitado	Permite las operaciones de invitado de máquina virtual que implican modificaciones en un sistema operativo invitado de una máquina virtual, como la transferencia de un archivo a la máquina virtual. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	Máquinas virtuales
Máquina virtual.Operaciones de invitado.Ejecución de programas de operaciones de invitado	Permite las operaciones de invitado de máquina virtual que implican ejecutar un programa en la máquina virtual. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	Máquinas virtuales
Máquina virtual.Operaciones de invitado.Consultas de operaciones de invitado	Permite las operaciones de invitado de máquina virtual que implican consultar el sistema operativo invitado, como enumerar archivos en el sistema operativo invitado. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	Máquinas virtuales

Privilegios para la interacción con máquinas virtuales

Estos privilegios controlan la capacidad de interactuar con la consola de una máquina virtual, configurar soportes físicos, realizar operaciones de energía e instalar VMware Tools.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-31. Interacción con la máquina virtual

Nombre del privilegio	Descripción	Necesario para
Máquina virtual .Interacción .Responder pregunta	Permite solucionar problemas con las transiciones de estados de las máquinas virtuales o con errores de tiempo de ejecución.	Máquinas virtuales
Máquina virtual .Interacción .Operación de copia de seguridad en máquina virtual	Permite realizar operaciones de copia de seguridad en las máquinas virtuales.	Máquinas virtuales
Máquina virtual .Interacción .Configurar medio de CD	Permite configurar un dispositivo virtual de DVD o CD-ROM.	Máquinas virtuales
Máquina virtual .Interacción .Configurar medio de disquete	Permite configurar un dispositivo virtual de disquete.	Máquinas virtuales
Máquina virtual .Interacción .Interacción de consola	Permite interactuar con el mouse, el teclado y la pantalla virtuales de las máquinas virtuales.	Máquinas virtuales
Máquina virtual .Interacción .Crear captura de pantalla	Permite crear una captura de pantalla de una máquina virtual.	Máquinas virtuales
Máquina virtual .Interacción .Desfragmentar todos los discos	Permite realizar operaciones de desfragmentación en todos los discos de la máquina virtual.	Máquinas virtuales
Máquina virtual .Interacción .Conexión de dispositivos	Permite cambiar el estado conectado de los dispositivos virtuales desconectables de una máquina virtual.	Máquinas virtuales
Máquina virtual .Interacción .Arrastrar y soltar	Permite arrastrar y soltar archivos entre una máquina virtual y un cliente remoto.	Máquinas virtuales
Máquina virtual .Interacción .Administración de sistema operativo invitado mediante VIX API	Permite administrar el sistema operativo de la máquina virtual mediante VIX API.	Máquinas virtuales
Máquina virtual .Interacción .Inyectar códigos de análisis de HID USB	Permite inyectar códigos de análisis de dispositivos USB HID.	Máquinas virtuales

Tabla 13-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Máquina virtual .Interacción .Pausar o cancelar la pausa	Permite poner en pausa la máquina virtual y anular la pausa.	Máquinas virtuales
Máquina virtual .Interacción .Realizar operaciones de borrado o reducción	Permite realizar operaciones de borrado o reducción en la máquina virtual.	Máquinas virtuales
Máquina virtual .Interacción .Apagar	Permite apagar una máquina virtual que se encuentra encendida. Esta operación apaga el sistema operativo invitado.	Máquinas virtuales
Máquina virtual .Interacción .Encender	Permite encender una máquina virtual que se encuentra apagada y reanudar una máquina virtual suspendida.	Máquinas virtuales
Máquina virtual .Interacción .Grabar sesión en máquina virtual	Permite grabar una sesión en una máquina virtual.	Máquinas virtuales
Máquina virtual .Interacción .Reproducir sesión en máquina virtual	Permite reproducir una sesión grabada en una máquina virtual.	Máquinas virtuales
Máquina virtual .Interacción .Restablecer	Permite restablecer una máquina virtual y reiniciar el sistema operativo invitado.	Máquinas virtuales
Máquina virtual .Interacción .Reanudar Fault Tolerance	Permite reanudar la tolerancia a errores en una máquina virtual.	Máquinas virtuales
Máquina virtual .Interacción .Suspender	Permite suspender una máquina virtual que se encuentra encendida. Esta operación pone al invitado en modo de espera.	Máquinas virtuales
Máquina virtual .Interacción .Suspender Fault Tolerance	Permite suspender la tolerancia a errores en una máquina virtual.	Máquinas virtuales
Máquina virtual .Interacción .Probar conmutación por error	Permite probar la conmutación por error de Fault Tolerance al convertir la máquina virtual secundaria en la máquina virtual principal.	Máquinas virtuales

Tabla 13-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Máquina virtual .Interacción .Probar reinicio de máquina virtual secundaria	Permite finalizar la máquina virtual secundaria de una máquina virtual mediante Fault Tolerance.	Máquinas virtuales
Máquina virtual .Interacción .Desactivar Fault Tolerance	Permite apagar Fault Tolerance en una máquina virtual.	Máquinas virtuales
Máquina virtual .Interacción .Activar Fault Tolerance	Permite encender Fault Tolerance en una máquina virtual.	Máquinas virtuales
Máquina virtual .Interacción .Instalar VMware Tools	Permite montar y desmontar el CD instalador de VMware Tools como CD-ROM del sistema operativo invitado.	Máquinas virtuales

Privilegios de inventario de máquinas virtuales

Los privilegios de inventario de máquinas virtuales controlan las operaciones de agregar, mover y eliminar máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-32. Privilegios de inventario de máquinas virtuales

Nombre del privilegio	Descripción	Necesario para
Máquina virtual .Inventario.Crear a partir de existente	Permite crear una máquina virtual a partir de una máquina virtual o plantilla existentes, mediante la clonación o la implementación desde una plantilla.	Clústeres, hosts, carpetas de máquina virtual
Máquina virtual .Inventario.Crear nuevo	Permite crear una máquina virtual y asignar recursos para su ejecución.	Clústeres, hosts, carpetas de máquina virtual
Máquina virtual .Inventario.Mover	Permite mover de lugar una máquina virtual en la jerarquía. El privilegio debe estar presente tanto en el origen como en el destino.	Máquinas virtuales
Máquina virtual .Inventario.Registrar	Permite agregar una máquina virtual existente a vCenter Server o al inventario de hosts.	Clústeres, hosts, carpetas de máquina virtual

Tabla 13-32. Privilegios de inventario de máquinas virtuales (continuación)

Nombre del privilegio	Descripción	Necesario para
Máquina virtual .Inventario.Eliminar	Permite eliminar una máquina virtual. Esta acción elimina del disco los archivos subyacentes de la máquina virtual. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Máquinas virtuales
Máquina virtual .Inventario.Eliminar del registro	Permite cancelar el registro de una máquina virtual de una instancia de vCenter Server o un inventario de host. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Máquinas virtuales

Privilegios de aprovisionamiento de las máquinas virtuales

Los privilegios de aprovisionamiento de las máquinas virtuales controlan las actividades relacionadas con la implementación y la personalización de las máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-33. Privilegios de aprovisionamiento de las máquinas virtuales

Nombre del privilegio	Descripción	Necesario para
Máquina virtual .Aprovisionamiento. Permitir acceso al disco	Permite abrir un disco en una máquina virtual con acceso aleatorio de lectura y escritura. Se utiliza sobre todo para el montaje de discos remotos.	Máquinas virtuales
Máquina virtual .Aprovisionamiento. Permitir acceso a archivos	Permite operaciones en archivos asociados con una máquina virtual, incluido vmx, discos, registros y nvram.	Máquinas virtuales
Máquina virtual .Aprovisionamiento. Permitir acceso de solo lectura al disco	Permite abrir un disco en una máquina virtual con acceso aleatorio de lectura. Se utiliza sobre todo para el montaje de discos remotos.	Máquinas virtuales
Máquina virtual .Aprovisionamiento. Permitir descarga de máquina virtual	Permite leer operaciones en archivos asociados con una máquina virtual, incluido vmx, discos, registros y nvram.	Host raíz o vCenter Server
Máquina virtual .Aprovisionamiento. Permitir carga de archivos de máquina virtual	Permite escribir operaciones en archivos asociados con una máquina virtual, incluido vmx, discos, registros y nvram.	Host raíz o vCenter Server
Máquina virtual .Aprovisionamiento. Clonar plantilla	Permite clonar una plantilla.	Plantillas

Tabla 13-33. Privilegios de aprovisionamiento de las máquinas virtuales (continuación)

Nombre del privilegio	Descripción	Necesario para
Máquina virtual .Aprovisionamiento. Clonar máquina virtual	Permite clonar una máquina virtual ya existente y asignar recursos.	Máquinas virtuales
Máquina virtual .Aprovisionamiento. Crear plantilla desde máquina virtual	Permite crear una plantilla nueva desde una máquina virtual.	Máquinas virtuales
Máquina virtual .Aprovisionamiento. Personalizar	Permite personalizar el sistema operativo invitado de una máquina virtual sin moverla.	Máquinas virtuales
Máquina virtual .Aprovisionamiento.Implementar plantilla	Permite implementar una máquina virtual desde una plantilla.	Plantillas
Máquina virtual .Aprovisionamiento. Marcar como plantilla	Permite marcar como una plantilla a una máquina virtual ya existente que está apagada.	Máquinas virtuales
Máquina virtual .Aprovisionamiento. Marcar como máquina virtual	Permite marcar una plantilla existente como una máquina virtual.	Plantillas
Máquina virtual .Aprovisionamiento. Modificar especificación de personalización	Permite crear, modificar o eliminar especificaciones de personalización.	vCenter Server raíz
Máquina virtual .Aprovisionamiento. Promover discos	Permite promover operaciones en los discos de una máquina virtual.	Máquinas virtuales
Máquina virtual .Aprovisionamiento. Leer especificaciones de personalización	Permite leer una especificación de personalización.	Máquinas virtuales

Privilegios de configuración de servicios de la máquina virtual

Los privilegios de configuración de servicios de la máquina virtual controlan quién puede realizar tareas de supervisión y administración en la configuración de servicios.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-34. Privilegios de configuración de servicios de la máquina virtual

Nombre del privilegio	Descripción
Máquina virtual. Configuración de servicios. Permitir notificaciones	Permite generar y recibir notificaciones sobre el estado del servicio.
Máquina virtual. Configuración de servicios. Permitir medición de notificaciones de eventos globales	Permite consultar si hay notificaciones presentes.
Máquina virtual. Configuración de servicios. Administrar configuración de servicios	Permite crear, modificar y eliminar servicios de la máquina virtual.
Máquina virtual. Configuración de servicios. Modificar configuración de servicios	Permite modificar la configuración actual del servicio de la máquina virtual.
Máquina virtual. Configuración de servicios. Consultar configuración de servicios	Permite recuperar la lista de servicios de la máquina virtual.
Máquina virtual. Configuración de servicios. Leer configuración de servicios	Permite recuperar la configuración actual del servicio de la máquina virtual.

Privilegios de administración de snapshots de las máquinas virtuales

Los privilegios de administración de snapshots de las máquinas virtuales controlan la capacidad para crear, eliminar, cambiar el nombre y restaurar snapshots.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-35. Privilegios del estado de las máquinas virtuales

Nombre del privilegio	Descripción	Necesario para
Máquina virtual .Administración de instantáneas. Crear instantánea	Permite crear una snapshot a partir del estado actual de la máquina virtual.	Máquinas virtuales
Máquina virtual .Administración de instantáneas.Eliminar instantánea	Permite quitar una snapshot del historial de snapshots.	Máquinas virtuales

Tabla 13-35. Privilegios del estado de las máquinas virtuales (continuación)

Nombre del privilegio	Descripción	Necesario para
Máquina virtual .Administración de instantáneas.Cambiar nombre de instantánea	Permite cambiar el nombre de una snapshot con un nuevo nombre, una nueva descripción o ambos.	Máquinas virtuales
Máquina virtual .Administración de instantáneas.Revertir a instantánea	Permite configurar la máquina virtual con el estado que tenía en una snapshot determinada.	Máquinas virtuales

Privilegios de vSphere Replication de máquinas virtuales

Los privilegios de vSphere Replication de máquinas virtuales controlan la utilización de la replicación que hace VMware vCenter Site Recovery Manager™ en máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-36. vSphere Replication de máquinas virtuales

Nombre del privilegio	Descripción	Necesario para
Máquina virtual .vSphere Replication.Configurar replicación	Permite configurar la replicación de la máquina virtual.	Máquinas virtuales
Máquina virtual .vSphere Replication.Administrar replicación	Permite activar la sincronización completa, en línea o sin conexión de una replicación.	Máquinas virtuales
Máquina virtual .vSphere Replication.Supervisar replicación	Permite supervisar la replicación.	Máquinas virtuales

Privilegios de grupo dvPort

Los privilegios de grupo de puertos virtuales distribuidos controlan la capacidad para crear, eliminar y modificar grupos de puertos virtuales distribuidos.

En la tabla se describen los privilegios necesarios para crear y configurar grupos de puertos virtuales distribuidos.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-37. Privilegios del grupo de puertos virtuales distribuidos

Nombre del privilegio	Descripción	Necesario para
Grupo de dvPorts.Crear	Permite crear un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales
Grupo de dvPorts.Eliminar	Permite eliminar un grupo de puertos virtuales distribuidos. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Grupos de puertos virtuales
Grupo de dvPorts.Modificar	Permite modificar la configuración de un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales
Grupo de dvPorts.Operación de directiva	Permite configurar la directiva de un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales
Grupo de dvPorts.Operación de ámbito	Permite configurar el ámbito de un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales

Privilegios de vApp

Los privilegios de vApp controlan las operaciones relacionadas con la implementación y la configuración de una vApp.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-38. Privilegios de vApp

Nombre del privilegio	Descripción	Necesario para
vApp.Agregar máquina virtual	Permite agregar una máquina virtual a una vApp.	vApps
vApp.Asignar grupo de recursos	Permite asignar un grupo de recursos a una vApp.	vApps
vApp.Asignar vApp	Permite asignar una vApp a otra vApp.	vApps
vApp.Clonar	Permite clonar una vApp.	vApps
vApp.Crear	Permite crear una vApp.	vApps
vApp.Eliminar	Permite eliminar una vApp. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	vApps
vApp.Exportar	Permite exportar una vApp desde vSphere.	vApps

Tabla 13-38. Privilegios de vApp (continuación)

Nombre del privilegio	Descripción	Necesario para
vApp.Importar	Permite importar una vApp a vSphere.	vApps
vApp.Mover	Permite mover una vApp a una nueva ubicación de inventario.	vApps
vApp.Apagar	Permite apagar las operaciones en una vApp.	vApps
vApp.Encender	Permite encender las operaciones en una vApp.	vApps
vApp.Cambiar nombre	Permite cambiarle el nombre a una vApp.	vApps
vApp.Suspender	Permite suspender una vApp.	vApps
vApp.Eliminar del registro	Permite anular el registro de una vApp. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	vApps
vApp.Ver entorno de OVF	Permite visualizar el entorno de OVF de una máquina virtual encendida dentro de una vApp.	vApps
vApp.Configuración de aplicaciones de vApp	Permite modificar la estructura interna de una vApp, como la información y las propiedades de un producto.	vApps
vApp.Configuración de instancias de vApp	Permite modificar la configuración de las instancias de una vApp, como sus directivas.	vApps
vApp.Configuración de managedBy de vApp	Permite que una extensión o una solución marque una vApp como administrada por ella. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	vApps
vApp.Configuración de recursos de vApp	Permite modificar la configuración de recursos de una vApp. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	vApps

Privilegios de vServices

Los privilegios de vServices controlan la capacidad para crear, configurar y actualizar dependencias de vService para máquinas virtuales y vApps.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-39. vServices

Nombre del privilegio	Descripción	Necesario para
vService.Crear dependencia	Permite crear una dependencia de vService para una máquina virtual o vApp.	vApps y máquinas virtuales
vService.Destruir dependencia	Permite quitar una dependencia de vService para una máquina virtual o vApp.	vApps y máquinas virtuales
vService.Volver a ajustar la configuración de dependencia	Permite volver a configurar una dependencia para actualizar el proveedor o la unión.	vApps y máquinas virtuales
vService.Actualizar dependencia	Permite actualizar una dependencia para configurar el nombre o la descripción.	vApps y máquinas virtuales

Privilegios de etiquetado de vSphere

Los privilegios de etiquetado de vSphere controlan la capacidad de crear y eliminar etiquetas y categorías de etiquetas, así como de asignar y quitar etiquetas en los objetos de inventario de vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 13-40. Privilegios de etiquetado de vSphere

Nombre del privilegio	Descripción	Necesario para
Etiquetado de vSphere.Asignar o desasignar etiqueta de vSphere	Permite asignar o anular la asignación de una etiqueta de un objeto en el inventario de vCenter Server.	Cualquier objeto
Etiquetado de vSphere.Crear etiqueta de vSphere	Permite crear una etiqueta.	Cualquier objeto
Etiquetado de vSphere.Crear categoría de etiqueta de vSphere	Permite crear una categoría de etiqueta.	Cualquier objeto
Etiquetado de vSphere.Crear ámbito de etiqueta de vSphere	Permite crear un ámbito de etiqueta.	Cualquier objeto
Etiquetado de vSphere.Eliminar etiqueta de vSphere	Permite eliminar una etiqueta.	Cualquier objeto
Etiquetado de vSphere.Eliminar categoría de etiqueta de vSphere	Permite eliminar una etiqueta.	Cualquier objeto
Etiquetado de vSphere.Eliminar ámbito de etiqueta de vSphere	Permite eliminar un ámbito de etiqueta.	Cualquier objeto
Etiquetado de vSphere.Editar etiqueta de vSphere	Permite editar una etiqueta.	Cualquier objeto
Etiquetado de vSphere.Editar categoría de etiqueta de vSphere	Permite editar una categoría de etiqueta.	Cualquier objeto

Tabla 13-40. Privilegios de etiquetado de vSphere (continuación)

Nombre del privilegio	Descripción	Necesario para
Etiquetado de vSphere.Editar ámbito de etiqueta de vSphere	Permite editar un ámbito de etiqueta.	Cualquier objeto
Etiquetado de vSphere.Modificar campo UsedBy por categoría	Permite cambiar el campo Usado por en una categoría de etiqueta.	Cualquier objeto
Etiquetado de vSphere.Modificar campo UsedBy por etiqueta	Permite cambiar el campo Usado por de una etiqueta.	Cualquier objeto

Descripción general de fortalecimiento y cumplimiento de vSphere

14

Se espera que las organizaciones reduzcan el riesgo de robo de datos, ataque cibernético o acceso no autorizado para proteger sus datos. Además, las organizaciones deben cumplir con los reglamentos de las normas gubernamentales y las normas privadas, como el Instituto nacional de normas y tecnología (National Institute of Standards and Technology, NIST) y las Guías de implementación técnica de seguridad (Security Technical Implementation Guides, STIG) de la Agencia de sistemas de información de defensa (Defense Information Systems Agency, DISA). Garantizar la conformidad de un entorno de vSphere con estas normas implica comprender un conjunto más amplio de consideraciones, incluidas personas, procesos y tecnología.

Una descripción general detallada de los temas de seguridad y conformidad que requieren atención permite planificar la estrategia de seguridad. También se pueden aprovechar otros recursos relacionados con la conformidad disponibles en el sitio web de VMware.

Este capítulo incluye los siguientes temas:

- Seguridad y conformidad en el entorno de vSphere
- Descripción general de la guía de configuración de seguridad de vSphere
- Acerca del Instituto nacional de estándares y tecnología
- Acerca de STIG de DISA
- Acerca del ciclo de vida de desarrollo de seguridad de VMware
- Registro de auditoría
- Descripción general de los próximos pasos de seguridad y conformidad

Seguridad y conformidad en el entorno de vSphere

Generalmente, los términos "seguridad" y "conformidad" se utilizan como sinónimos. Sin embargo, son conceptos únicos y distintos.

La seguridad, que normalmente se piensa como seguridad de la información, se define como un conjunto de controles técnicos, físicos y administrativos que se implementan para proporcionar confidencialidad, integridad y disponibilidad. Por ejemplo, para proteger un host, se bloquean las cuentas que pueden iniciar sesión en el host y el medio por el cual pueden hacerlo (SSH, consola directa, etc.). La conformidad, por el contrario, es un conjunto de requisitos necesarios para cumplir con los controles mínimo establecidos por diferentes marcos normativos en los

que se proporcionan directrices limitadas sobre un tipo específico de tecnología, proveedor o configuración. Por ejemplo, la industria de tarjetas de pago (Payment Card Industry, PCI) establece directrices de seguridad para ayudar a las organizaciones a proteger proactivamente los datos de las cuentas de clientes.

La seguridad reduce el riesgo de robo de datos, ataque cibernético o acceso no autorizado, mientras que la conformidad es la prueba de que un control de seguridad está en vigor, por lo general, dentro de una línea de tiempo definida. La seguridad se expone principalmente en las decisiones de diseño y se destaca dentro de las configuraciones de tecnología. La conformidad se centra en trazar la correlación entre los controles de seguridad y los requisitos específicos. Un mapa de conformidad proporciona una vista centralizada para enumerar muchos de los controles de seguridad requeridos. Esos controles se describen más detalladamente cuando se incluyen las respectivas citas de conformidad de cada control de seguridad según lo indica un dominio como NIST, PCI, FedRAMP, HIPAA, etc.

Los programas efectivos de conformidad y ciberseguridad se basan en tres pilares: personas, procesos y tecnología. Un error de concepto general es que solo la tecnología puede resolver todas las necesidades de ciberseguridad. La tecnología desempeña un papel importante y amplio en el desarrollo y la ejecución de un programa de seguridad de la información. Sin embargo, si la tecnología no cuenta con procesos y procedimientos, conocimientos y formación, genera una vulnerabilidad dentro de la organización.

Al definir las estrategias de seguridad y conformidad, tenga en cuenta lo siguiente:

- Las personas necesitan formación y conocimientos generales, mientras que el personal de TI necesita formación específica.
- El proceso define la forma en que se utilizan las actividades, los roles y la documentación de la organización para mitigar el riesgo. Los procesos solo son efectivos si las personas los siguen correctamente.
- La tecnología puede utilizarse para prevenir o reducir el impacto de los riesgos de ciberseguridad sobre la organización. La tecnología que se utiliza depende del nivel de aceptación de riesgos de la organización.

VMware proporciona kits de conformidad que contienen una guía de auditoría y una guía de aplicabilidad de productos, lo que ayuda a puentear la brecha entre los requisitos de conformidad y normativas y las guías de implementación. Para obtener más información, consulte https://core.vmware.com/compliance.

Glosario de términos de conformidad

La conformidad introduce términos y definiciones específicos que es importante comprender.

Tabla 14-1. Términos de conformidad

Término	Definición
CJIS	Servicios de información de justicia penal. En el contexto de la conformidad, CJIS desarrolla una directiva de seguridad sobre la forma en que la justicia penal local, estatal y federal y los organismos de seguridad deben tomar precauciones de seguridad para proteger la información confidencial, como las huellas digitales y los antecedentes penales.
STIG de DISA	Guía de implementación técnica de seguridad de la Agencia de sistemas de información de defensa. La Agencia de Sistemas de Información de Defensa (Defense Information Systems Agency, DISA) es la entidad responsable de mantener la posición de seguridad de la infraestructura de TI del Departamento de Defensa (Department of Defense, DoD). DISA lleva a cabo esta tarea mediante el desarrollo y el uso de guías de implementación técnica de seguridad (Security Technical Implementation Guides, STIG).
FedRAMP	Programa federal de administración de riesgos y autorizaciones. FedRAMP es un programa gubernamental con un enfoque estandarizado para la evaluación, la autorización y la supervisión continua de la seguridad de los productos y servicios de nube.
HIPAA	Ley de transferencia y responsabilidad de seguro médico. Aprobada en el congreso en 1996, la ley HIPAA hace lo siguiente: ■ Otorga a millones de trabajadores norteamericanos y sus familias la capacidad de transferir y continuar con la cobertura de seguro médico cuando cambian su trabajo o lo pierden. ■ Reduce los fraudes y los abusos en atención médica. ■ Impone normas para todo el sector sobre la información de atención médica en la facturación electrónica y otros procesos. ■ Requiere la protección y la manipulación confidencial de la información de salud protegida. La última viñeta es de máxima importancia para la documentación *Seguridad de vSphere*.
NCCoE	Centro Nacional de Excelencia en Ciberseguridad. NCCoE es una organización gubernamental de Estados Unidos que produce y comparte públicamente soluciones para los problemas de ciberseguridad que padecen las empresas norteamericanas. El centro forma un equipo con personal de empresas de tecnología de ciberseguridad, otros organismos federales y la comunidad académica para abordar cada problema.

Tabla 14-1. Términos de conformidad (continuación)

Término	Definición
NIST	Instituto nacional de normas y tecnología. Fundado en 1901, el NIST es un organismo federal no regulador dentro del Departamento de comercio de Estados Unidos. La misión de NIST es fomentar la innovación y la competitividad industrial de Estados Unidos mediante la promoción de normas, tecnologías y ciencias de la medición con el fin de aumentar la seguridad económica y mejorar nuestra calidad de vida.
PAG	Guía de aplicabilidad de productos. Este documento proporciona directrices generales para las organizaciones que están considerando usar soluciones de una empresa con el fin de abordar sus requisitos de conformidad.
DSS de PCI	Estándar de seguridad de datos para la Industria de tarjeta de pago. Un conjunto de normas de seguridad diseñadas para garantizar que todas las empresas que acepten, procesen, almacenen o transmitan información de tarjetas de crédito mantengan un entorno seguro.
Soluciones de cumplimiento de VVD/VCF	VMware Validated Designs/VMware Cloud Foundation. VMware Validated Designs proporciona proyectos integrales exhaustivamente probados para crear y operar un centro de datos definido por software. Con las soluciones de conformidad de VVD/VCF, los clientes pueden cumplir con los requisitos de conformidad de varios reglamentos de la industria y del gobierno.

Descripción general de la guía de configuración de seguridad de vSphere

VMware crea guías de fortalecimiento de seguridad que proporcionan instrucciones prescriptivas para implementar y operar los productos de VMware de forma segura. Para vSphere, esta guía se denomina *Guía de configuración de seguridad de vSphere* (anteriormente conocida como *Guía de fortalecimiento*).

La *Guía de configuración de seguridad de vSphere* contiene las prácticas recomendadas de seguridad para vSphere. La *Guía de configuración de seguridad de vSphere* no se relaciona directamente con directrices o marcos normativos, por lo que no es una guía de cumplimiento. Además, la *Guía de configuración de seguridad de vSphere* no está diseñada para usarse como lista de comprobación de seguridad. La seguridad siempre implica ceder en algo. Implementar controles de seguridad puede afectar negativamente la facilidad de uso, el rendimiento u otras tareas operativas. Tenga en cuenta las cargas de trabajo, los patrones de uso, la estructura organizativa, entre otros elementos, antes de realizar cambios de seguridad, ya sea que los consejos provengan de VMware o de otras fuentes del sector. Si su organización tiene necesidades de conformidad normativa, consulte Seguridad y conformidad en el entorno de vSphere o visite https://core.vmware.com/compliance. Este sitio incluye kits de conformidad y

guías de auditoría de productos para ayudar a los administradores de vSphere y a los auditores normativos a garantizar y dar fe de la conformidad de la infraestructura virtual en cuanto a los marcos normativos, como NIST 800-53v4, NIST 800-171, PCI DSS, HIPAA, CJIS, ISO 27001, entre otros.

La *Guía de configuración de seguridad de vSphere* no analiza la protección de los siguientes elementos:

- Software que se ejecuta dentro de la máquina virtual, como el sistema operativo invitado y las aplicaciones
- Tráfico que se ejecuta a través de las redes de máquina virtual
- Seguridad de los productos de extensión

La *Guía de configuración de seguridad de vSphere* no se creó para ser usada como una herramienta de "conformidad". La *Guía de configuración de seguridad de vSphere* permite dar los primeros pasos hacia el cumplimiento, pero no garantiza que la implementación sea conforme por sí misma. Para obtener más información sobre la conformidad, consulte Seguridad y conformidad en el entorno de vSphere.

Leer la Guía de configuración de seguridad de vSphere

La *Guía de configuración de seguridad de vSphere* es una hoja de cálculo con directrices de seguridad de ayuda para modificar la configuración de seguridad de vSphere. Estas directrices se agrupan en pestañas en función de los componentes afectados, con algunas de las siguientes columnas o todas ellas.

Tabla 14-2. Columnas de la hoja de cálculo Guía de configuración de seguridad de vSphere

Encabezado de columna	Descripción
Identificador de directriz	Un identificador único de dos partes para hacer referencia a una recomendación de fortalecimiento o una configuración de seguridad. La primera parte indica el componente, que se define de la siguiente manera: ■ ESXi: hosts ESXi ■ VM: máquinas virtuales ■ vNetwork: conmutadores virtuales
Descripción	Una breve explicación de la recomendación determinada.
Discusión	Un descripción de la vulnerabilidad detrás de una recomendación determinada.
Parámetro de configuración	El parámetro de configuración aplicable o el nombre de archivo, si existe alguno.

Tabla 14-2. Columnas de la hoja de cálculo Guía de configuración de seguridad de vSphere (continuación)

Encabezado de columna	Descripción
Valor deseado	El estado o valor deseado de la recomendación. Los posibles valores son: ■ N/C ■ Específico del sitio ■ False ■ True ■ Habilitado ■ Deshabilitado ■ No presente o Falso
Valor predeterminado	El valor predeterminado establecido por vSphere.
¿Es el valor deseado el predeterminado?	Indica si el ajuste de seguridad es la configuración predeterminada del producto.
Acción necesaria	El tipo de acción que se realizará en la recomendación determinada. Las acciones incluyen: ■ Actualizar ■ Solo auditoría ■ Modificar ■ Agregar ■ Quitar
Establecer la ubicación en vSphere Client	Los pasos para comprobar el valor mediante vSphere Client.
¿Impacto funcional negativo al cambiar el valor predeterminado?	La descripción, si existe una, de un impacto potencial negativo por usar la recomendación de seguridad.
Evaluación mediante comandos de PowerCLI	Los pasos para comprobar el valor mediante PowerCLI.
Ejemplo de corrección mediante un comando de PowerCLI	Los pasos para establecer (corregir) el valor mediante PowerCLI.
Corrección mediante comandos de vCLI	Los pasos para configurar (corregir) el valor mediante comandos de vCLI.
Evaluación mediante comandos de PowerCLI	Los pasos para comprobar el valor mediante comandos de PowerCLI.
Corrección mediante comandos de PowerCLI	Los pasos para configurar (corregir) el valor mediante comandos de PowerCLI.
Se puede establecer mediante el perfil de host	Si la configuración se puede realizar mediante perfiles de host (se aplica solo a las directrices de ESXi).
Fortalecimiento	Si es TRUE, la directriz tiene solo una implementación que sea conforme. Si es FALSE, se puede cumplir con la implementación de la directriz con más de una opción de configuración. A menudo, el valor real es específico del sitio.

Tabla 14-2. Columnas de la hoja de cálculo Guía de configuración de seguridad de vSphere (continuación)

Encabezado de columna	Descripción
Ajuste específico del sitio	Si es TRUE, el ajuste conforme con la directriz depende de reglas o normas que son específicas para esa implementación de vSphere.
Ajuste de auditoría	Si es TRUE, es posible que el valor del ajuste enumerado deba ser modificado para cumplir con las reglas específicas del sitio.

Nota Estas columnas pueden cambiar con el paso del tiempo según sea necesario. Por ejemplo, algunas adiciones recientes son las columnas Identificador de STIG de DISA, Fortalecimiento y Ajuste específico del sitio. Consulte https://blogs.vmware.com para ver anuncios sobre las actualizaciones de la *Guía de configuración segura de vSphere*.

No aplique ciegamente las directrices de la *Guía de configuración segura de vSphere* en su entorno. En cambio, dedique un momento a evaluar cada ajuste y tome una decisión informada sobre si aplicarlo o no. Como mínimo, puede utilizar las instrucciones de las columnas Evaluación para comprobar la seguridad de su implementación.

La *Guía de configuración segura de vSphere* es una ayuda para comenzar a aplicar la conformidad en la implementación. Cuando se utiliza con las guías de DISA y otras directrices de conformidad, la *Guía de configuración segura de vSphere* permite asignar los controles de seguridad de vSphere según el tipo de conformidad de cada directriz.

Acerca del Instituto nacional de estándares y tecnología

El instituto nacional de estándares y tecnología (National Institute of Standards and Technology, NIST) es un organismo público no regulador que desarrolla tecnología, métricas, estándares y directrices. La conformidad con estándares y directrices de NIST actualmente se ha convertido en una prioridad para muchos sectores.

El NIST se fundó en 1901 y ahora forma parte del departamento de comercio de EE. UU. El NIST es uno de los laboratorios de ciencias físicas más antiguos del país. Hoy en día, las mediciones del NIST admiten desde las tecnologías más pequeñas hasta las más grandes y complejas de las creaciones humanas, ya sean dispositivos a nanoescala, rascacielos antisísmicos o redes de comunicación global.

La Ley Federal de Administración de la Seguridad de la Información (Federal Information Security Management Act, FISMA) es una ley federal de Estados Unidos promulgada en 2002 a partir de la cual es un requisito que las agencias federales desarrollen, documenten e implementen un programa de seguridad y protección de la información. El NIST desempeña un papel importante en la implementación de la ley FISMA, ya que produce estándares y directrices de seguridad de claves (por ejemplo, FIPS 199, FIPS 200 y la serie SP 800).

El gobierno y las organizaciones privadas utilizan la base de datos NIST 800-53 para proteger los sistemas de información. La ciberseguridad y los controles de privacidad son esenciales para proteger las operaciones organizativas (incluidas su misión, sus funciones, su imagen y su reputación), los activos de la organización y a usuarios individuales frente a una amplia variedad de amenazas. Algunas de estas amenazas incluyen ataques cibernéticos hostiles, catástrofes naturales, fallas estructurales y errores humanos. VMware ha inscrito a un partner de auditoría externo para evaluar los productos y las soluciones de VMware mediante el catálogo de controles NIST 800-53. Para obtener más información, visite la página web del NIST en https://www.nist.gov/cyberframework.

Acerca de STIG de DISA

La Agencia de Sistemas de Información de Defensa (Defense Information Systems Agency, DISA) desarrolla y publica las guías de implementación técnica de seguridad (Security Technical Implementation Guides, STIG). Las STIG de DISA proporcionan instrucciones técnicas para fortalecer los sistemas y reducir las amenazas.

DISA es la agencia de apoyo de combate del DoD de EE. UU., responsable de mantener la posición de seguridad de la red de información del DoD (DoD Information Network, DODIN). Una de las formas en que DISA lleva a cabo esta tarea es desarrollando, difundiendo y exigiendo la implementación de STIG. En resumen, las STIG son guías portátiles basadas en estándares para fortalecer los sistemas. Las STIG son obligatorias para los sistemas de TI del DoD de EE. UU. y, como tales, proporcionan una línea base segura y verificada que permite a las entidades ajenas al DoD medir su situación de seguridad.

Los proveedores, como VMware, envían sugerencias para el refuerzo de la seguridad a la DISA para su evaluación, basándose en los protocolos y los comentarios de la DISA. Una vez completado ese proceso, se publica la STIG oficial en el sitio web de la organización DISA en https://public.cyber.mil/stigs/. Como parte de la *Guía de configuración de seguridad de vSphere*, VMware proporciona líneas base de seguridad y orientación para mejorar el fortalecimiento de vSphere. Consulte https://core.vmware.com/security.

Acerca del ciclo de vida de desarrollo de seguridad de VMware

El programa de ciclo de vida de desarrollo de seguridad (Security Development Lifecycle, SDL) de VMware identifica y reduce los riesgos para la seguridad durante la fase de desarrollo de los productos de software de VMware. VMware también opera el centro de respuestas de seguridad de VMware (VMware Security Response Center, VSRC) para llevar a cabo el análisis y la corrección de problemas de seguridad de software en los productos de VMware.

SDL es la metodología de desarrollo de software que el grupo de ingeniería de seguridad, comunicación y respuestas de VMware (VMware Security Engineering, Communication, and Response, vSECR) y los grupos de desarrollo de productos de VMware usan para ayudar a identificar y mitigar los problemas de seguridad. Para obtener más información sobre el ciclo de vida de desarrollo de seguridad de VMware, consulte la página web en https://www.vmware.com/security/sdl.html.

El VSRC trabaja con los clientes y la comunidad de investigación de seguridad para lograr los objetivos de solución de problemas de seguridad y para proporcionar a los clientes información práctica de seguridad de manera oportuna. Para obtener más información sobre el centro de respuestas de seguridad de VMware, consulte la página web en https://www.vmware.com/security/vsrc.html.

Registro de auditoría

El registro de auditoría de tráfico de red, alertas de conformidad, actividad del firewall, cambios del sistema operativo y actividades de aprovisionamiento se considera una práctica recomendada para mantener la seguridad de cualquier entorno de TI. Además, el registro es un requisito específico de muchas de las normas y los estándares.

Uno de los primeros pasos para garantizar que se está al tanto de los cambios en la infraestructura es auditar el entorno. De forma predeterminada, vSphere incluye herramientas que permiten ver y realizar un seguimiento de los cambios. Por ejemplo, puede utilizar la pestaña Tareas y eventos en vSphere Client para cualquier objeto en la jerarquía de vSphere a fin de ver los cambios producidos. También puede usar PowerCLI para recuperar eventos y tareas. Además, vRealize Log Insight ofrece el registro de auditoría para admitir la recopilación y retención de eventos importantes del sistema. Además, hay muchas herramientas de terceros disponibles que proporcionan auditoría de vCenter.

Los archivos de registro pueden proporcionar una traza de auditoría para ayudar a determinar quién o qué tiene acceso a un host, una máquina virtual, etc. Para obtener más información, consulte Ubicaciones de archivos de registro de ESXi.

Eventos de auditoría de Single Sign-On

Los eventos de auditoría de Single Sign-On (SSO) son registros de acciones del usuario o del sistema para obtener acceso a los servicios de SSO.

vCenter Server 6.7 Update 2 y versiones posteriores mejora la auditoría de VMware vCenter Single Sign-On al agregar eventos para las siguientes operaciones:

- Administración de usuarios
- Inicio de sesión
- Creación de grupos
- Origen de identidad
- Actualizaciones de directivas

Los orígenes de identidades compatibles son vsphere.local, autenticación integrada de Windows (Integrated Windows Authentication, IWA) y Active Directory en LDAP.

Cuando un usuario inicia sesión en vCenter Server a través de Single Sign-On, o realiza cambios que afectan a SSO, se escriben los siguientes eventos de auditoría en el archivo de registro de auditoría de SSO:

- **Intentos de inicio y cierre de sesión:** los eventos para todas las operaciones de inicio y cierre de sesión correctas y con errores.
- **Cambio de privilegio:** los eventos de cambio en el rol o los permisos de un usuario.
- **Cambio de cuenta:** los eventos de cambio en la información de la cuenta de usuario, por ejemplo, nombre de usuario, contraseña u otra información adicional de la cuenta.
- **Cambio de seguridad:** los eventos de cambio en una configuración, un parámetro o una directiva de seguridad.
- **Cuenta habilitada o deshabilitada:** los eventos para cuando se habilita o se deshabilita una cuenta.
- **Origen de identidad:** los eventos para agregar, eliminar o editar un origen de identidad.

En vSphere Client y vSphere Web Client, los datos de eventos se muestran en la pestaña **Supervisar**. Consulte la documentación de *Supervisión y rendimiento de vSphere*.

Nota La capacidad de ver los eventos mediante uno de los clientes de GUI solo está habilitada para vCenter Server Appliance.

Los datos de eventos de auditoría de SSO incluyen los siguientes detalles:

- Marca de tiempo de cuando se produjo el evento.
- Usuario que realizó la acción.
- Descripción del evento.
- Gravedad del evento.
- Dirección IP del cliente utilizado para conectarse a vCenter Server, si está disponible.

Descripción general del registro de eventos de auditoría de SSO

El proceso de Single Sign-On de vSphere escribe los eventos de auditoría en el archivo `audit_events.log` en las siguientes ubicaciones.

Tabla 14-3. Ubicación del registro de auditoría de SSO

Sistema operativo	Ubicación
vCenter Server Appliance	`/var/log/audit/sso-events/`
vCenter Server Windows	`C:\ProgramData\VMware\vCenterServer\runtime\VMwareSTSService\logs\`

Precaución Nunca edite manualmente el archivo `audit_events.log`, ya que esto puede provocar un error en el registro de auditoría.

Al trabajar con el archivo `audit_events.log`, tenga en cuenta lo siguiente:

- El archivo de registro se archiva al alcanzar 50 MB.
- Se conservan 10 archivos de almacenamiento como máximo. Si se alcanza el límite, el archivo más antiguo se depura al crear un nuevo archivo.
- Los archivos llevan el nombre `audit_events`-<índice>`.log.gz`, donde el índice es un número del 1 al 10. El primer archivo que se crea es el índice 1 y ese número aumenta con cada archivo subsiguiente.
- Los eventos más antiguos se encuentran en el índice 1 del archivo. El archivo con el índice más alto es el archivo más reciente.

Descripción general de los próximos pasos de seguridad y conformidad

Llevar a cabo una evaluación de seguridad es el primer paso para la comprensión de las vulnerabilidades en la infraestructura. Una evaluación de seguridad forma parte de una auditoría de seguridad, en la que se analizan sistemas y prácticas, incluida la conformidad de seguridad.

Por lo general, una evaluación de seguridad hace referencia a examinar la infraestructura física de una organización (firewalls, redes, hardware, etc.) para identificar vulnerabilidades y defectos. Una evaluación de seguridad no es lo mismo que una auditoría de seguridad. Una auditoría de seguridad no solo abarca una revisión de la infraestructura física, sino también otras áreas como las directivas y los procedimientos operativos estándar, incluida la conformidad de seguridad. Una vez obtenida la auditoría, es posible decidir los pasos para solucionar los problemas dentro del sistema.

Durante la preparación para realizar una auditoría de seguridad, se pueden realizar estas preguntas generales:

1 ¿Nuestra organización tiene la obligación de seguir una norma de cumplimiento? De ser así, ¿cuál?

2 ¿Cuál es nuestro intervalo de auditoría?

3 ¿Cuál es nuestro intervalo de autoevaluación interna?

4 ¿Tenemos acceso a los resultados de auditoría anteriores y los hemos visto?

5 ¿Utilizamos una empresa de auditoría externa para prepararnos para una auditoría? De ser así, ¿cuál es su nivel de comodidad con la virtualización?

6 ¿Ejecutamos análisis de vulnerabilidad en los sistemas y las aplicaciones? ¿Cuándo y con qué frecuencia?

7 ¿Cuáles son nuestras directivas de ciberseguridad internas?

8 ¿El registro de auditoría se configuró según sus necesidades? Consulte Registro de auditoría.

Si no existen instrucciones específicas o directrices sobre dónde empezar, es posible iniciar la protección del entorno de vSphere mediante las siguientes acciones:

- Mantener el entorno actualizado con las revisiones de software y firmware más recientes
- Mantener un nivel apropiado de protección y administración de contraseñas para todas las cuentas
- Revisar las recomendaciones de seguridad aprobadas por los proveedores
- Consultar las guías de configuración de seguridad de VMware (consulte Descripción general de la guía de configuración de seguridad de vSphere)
- Utilizar las instrucciones disponibles y comprobadas de marcos de directivas como NIST, ISO, etc.
- Seguir las instrucciones de los marcos de conformidad normativa como PCI, DISA y FedRAMP